MÉMORIAL DES SCIENCES MATHÉMATIQUES

J. HERBRAND

Le développement moderne de la théorie des corps algébriques

Mémorial des sciences mathématiques, fascicule 75 (1936)
<http://www.numdam.org/item?id=MSM_1936__75__1_0>

© Gauthier-Villars, 1936, tous droits réservés.

L'accès aux archives de la collection « Mémorial des sciences mathématiques » implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM
Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

BSM 14622

MÉMORIAL

DES

SCIENCES MATHÉMATIQUES

PUBLIÉ SOUS LE PATRONAGE DE

L'ACADÉMIE DES SCIENCES DE PARIS,

DES ACADÉMIES DE BELGRADE, BRUXELLES, BUCAREST, COÏMBRE, CRACOVIE, KIEW, MADRID, PRAGUE, ROME, STOCKHOLM (FONDATION MITTAG-LEFFLER), DE LA SOCIÉTÉ MATHÉMATIQUE DE FRANCE, AVEC LA COLLABORATION DE NOMBREUX SAVANTS

DIRECTEUR :

Henri VILLAT

Membre de l'Institut,
Professeur à la Sorbonne,
Directeur du « Journal de Mathématiques pures et appliquées »,

---

FASCICULE LXXV

Le développement moderne de la théorie des corps algébriques

Corps de classes et lois de réciprocité

Par M. J. HERBRAND

PARIS
GAUTHIER-VILLARS, ÉDITEUR
LIBRAIRE DU BUREAU DES LONGITUDES, DE L'ÉCOLE POLYTECHNIQUE
Quai des Grands-Augustins, 55.

1936

UNIVERSITÉ DE GRENOBLE I
LABORATOIRE
DE MATHÉMATIQUES PURES

AVERTISSEMENT

La Bibliographie est placée à la fin du fascicule, immédiatement avant la Table des Matières.

Les numéros en caractères gras, figurant entre crochets dans le courant du texte, renvoient à cette Bibliographie.

LE DÉVELOPPEMENT MODERNE

DE LA

THÉORIE DES CORPS ALGÉBRIQUES

CORPS DE CLASSES ET LOIS DE RÉCIPROCITÉ

Par M. J. HERBRAND ([1*]).

INTRODUCTION.

Depuis les recherches de Hilbert, il y a plus de 30 ans, la théorie des corps algébriques s'est développée sous le signe de la théorie du corps de classes, c'est-à-dire des corps dont le groupe de Galois par rapport à un domaine de rationalité est abélien, et il n'y eut que peu de travaux importants en dehors de cette direction. Son origine remonte aux travaux de Gauss sur les formes quadratiques, dans les célèbres *Disquitiones Arithmeticae;* dès cette époque, où la théorie des idéaux n'était pas connue, il a reconnu le lien qui existe entre la théorie des genres et les lois de réciprocité. La loi de réciprocité quadratique de Gauss et Legendre fut ensuite généralisée par Eisenstein et Kummer à qui est due la notation d'idéal. Mais ce fut Hilbert qui, le premier, reconnut que ces travaux épars devaient se réunir en un vaste édifice, la théorie du corps de classes. Il étudia à fond certains cas particuliers, et annonça que les mêmes méthodes devaient conduire au but dans le cas général. La plus grande partie des résultats annoncés par Hilbert fut ensuite démontrée par Furtwängler. Dans un autre domaine se poursuivait aussi l'étude de

([1*]) La mort tragique de J. Herbrand l'a empêché de relire lui-même les épreuves de ce fascicule. Elles ont été revues par C. Chevalley, qui a ajouté des notes, qui sont désignées par un *, et un appendice relatif aux progrès récents de la théorie.

la théorie du corps de classes, celui de la multiplication complexe des fonctions elliptiques, mais on y rencontrait les plus grandes difficultés. Ce ne fut qu'en 1920 que le mathématicien japonais Takagi, par un emploi heureux des notions introduites jusque-là et un remaniement complet de la théorie, réussit à développer jusqu'au bout la pensée de Hilbert, et à résoudre toutes les difficultés. Des compléments très importants furent ensuite apportés par Artin et Hasse.

L'état de la théorie des corps algébriques avait été exposé en 1896 par Hilbert [1] dans un ouvrage magistral; Hasse [2, 3, 4] a accompli une œuvre analogue pour celle du corps de classes, et c'est une chance unique que d'avoir dans ces délicates théories ces deux œuvres comme guides; elles contiennent en effet un exposé systématique et complet de toutes nos connaissances dans ces questions.

Citons encore un livre de Hecke [1] qui présente les bases de la théorie des corps algébriques sous une forme plus simple et souvent plus générale que l'ouvrage très dense et ardu de Hilbert.

La théorie du corps de classes a une réputation de difficulté qui est en partie justifiée. Mais il faut faire une distinction : il n'est peut-être pas en effet dans la science de théorie où tout à la fois les démonstrations soient aussi ardues, et les résultats d'une aussi parfaite simplicité et d'une aussi grande puissance. La difficulté des démonstrations ne résulte pas d'ailleurs de la complexité de leur structure logique, mais bien plutôt du fait qu'à chaque pas on a besoin de formules précises, dont l'établissement demande à chaque fois des calculs longs et délicats. D'ailleurs des travaux récents et encore inédits ont réalisé des simplifications considérables (1*).

Le but propre de ce fascicule est d'exposer la théorie du corps de classes; mais pour qu'il fut accessible au lecteur ne connaissant que peu de choses en théorie des nombres, nous avons résumé dans le premier Chapitre tout ce qu'il est nécessaire de savoir de la théorie générale des corps algébriques; nous n'avons pas craint d'aller jusqu'à rappeler les faits fondamentaux de la théorie des groupes et de la théorie de Galois. Nous avons évidemment présenté ces préliminaires de façon à faire ressortir ce qui était nécessaire pour la

(1*) J. Herbrand fait ici allusion aux travaux de lui-même (Herbrand [5], Artin [9], Hasse [25]), Artin [9], Hasse [25], Chevalley [4, 5, 6].

suite, mais nous nous sommes aussi efforcé de n'oublier aucun fait important, de manière à ce que l'on trouve là un résumé complet de la théorie. Notre but serait atteint si ces précautions pouvaient faciliter la tâche de quelques lecteurs et leur donner l'envie d'étudier de plus près ces théories, qui sont parmi les plus achevées de celles que nous présente la Science mathématique.

CHAPITRE I.

LA THÉORIE GÉNÉRALE DES CORPS ALGÉBRIQUES.

I. — Groupes.

Pour un exposé très élémentaire de la théorie des groupes on peut consulter Hasse [1], pour un exposé plus complet Speiser [1] ou Burnside [1].

1. Considérons un ensemble (fini ou infini) d'éléments dont la nature est pour le moment indéterminée, et une opération qui, à tout couple d'éléments a et b pris dans cet ordre, fait correspondre un troisième élément que l'on désignera en général par ab, dit *produit* de a et de b.

Supposons que les conditions suivantes sont réalisées :

1° $$a(bc) = (ab)c;$$

2° Il y a un élément e (dit *unité du groupe*) tel que, pour tout a,

$$ae = ea = a;$$

3° A tout élément x correspond un autre élément y tel que

$$xy = e.$$

Alors on dit que l'ensemble de ces éléments forme un *groupe* (*par rapport à cette opération*).

On démontre alors qu'il y a toujours pour tout a et tout b un élément x et un seul tel que $ax = b$, et un élément y et un seul tel que $ya = b$. Il faut remarquer qu'en général dans un groupe, xy et yx sont différents.

Si le nombre n des éléments d'un groupe G est fini, ce groupe est dit *fini;* ce nombre n est dit l'*ordre* du groupe; on écrit $n = (G)$.

L'élément x tel que $ax = e$ est dit l'inverse de a, et se désigne par a^{-1}; on a aussi $a^{-1}a = e$. On écrit par convention $aa = a^2$, $a^2 a = a^3, \ldots, a^{-1}a^{-1} = a^{-2}$, en général $a^m a^n = a^{m+n}$ (m et n étant des entiers positifs ou négatifs).

Les nombres rationnels positifs forment par exemple un groupe par rapport à la multiplication, où l'unité est 1; les entiers positifs, nul et négatifs, un groupe par rapport à l'addition, où l'unité est 0. Il nous arrivera plusieurs fois de considérer des groupes de nombres par rapport à l'addition; dans ce cas, l'unité est 0, le « produit » au sens de la théorie des groupes, de a et de b est $a + b$; nous conserverons dans ce cas la notation additive; en particulier, au lieu de a^m, nous écrirons ma. Dans le cas de groupes de nombres par rapport à la multiplication, la notation habituelle coïncide avec celle de la théorie des groupes.

2. Un groupe G est *isomorphe* à un groupe H si, à tout élément de H on peut faire correspondre un élément de G, de manière que si à x et y de H correspondent a et b de G, à xy corresponde ab (1*).

Cette correspondance est dite une *isomorphie*.

Si en particulier à deux éléments différents de H correspondent toujours deux éléments différents de G, les groupes sont dits *holoédriquement isomorphes*, et l'on écrit $G \simeq H$; cette relation est réciproque et transitive; et deux tels groupes peuvent être considérés comme identiques.

Désormais quand nous parlerons de groupes isomorphes, nous sous-entendrons « holoédriquement »; quand il n'en sera pas ainsi, nous parlerons de groupes *mériédriquement isomorphes* (2*).

3. Soit G un groupe, g un ensemble d'éléments de G formant aussi un groupe, g est dit un *sous-groupe* de G. Si G est fini, g forme un sous-groupe, sous la seule condition que, quand a et b sont dans g, ab y soit aussi. L'ordre de G est un multiple de celui de g.

σ étant un élément de G, $\alpha_i (i = 1, 2, \ldots, n)$ les éléments de g, les

(1*) Et que de plus tout élément de G soit le correspondant d'un élément de H.

(2*) Rappelons que l'on dit souvent « *homomorphe* » au lieu de mériédriquement isomorphe.

$\sigma\alpha_i\sigma^{-1}$ forment un nouveau groupe désigné par $\sigma g \sigma^{-1}$; g et tous ces groupes $\sigma g \sigma^{-1}$ sont dits *conjugués* entre eux. Si un groupe est identique à ses conjugués, il est dit *invariant*.

Supposons maintenant g invariant; deux éléments α et β de G sont dits *congrus* par rapport à g, s'il y a un élément x de g tel que $\alpha x = \beta$ (ou, ce qui revient au même, s'il y a un élément x de g tel que $x\alpha = \beta$). On écrit alors $\alpha \equiv \beta \pmod{g}$. On voit sans peine que :

1° Si $\alpha \equiv \beta \pmod{g}$, alors $\beta \equiv \alpha \pmod{g}$;
2° Si $\alpha \equiv \beta \pmod{g}$ et $\beta \equiv \gamma \pmod{g}$, alors $\alpha \equiv \gamma \pmod{g}$;
3° Si $\alpha \equiv \beta \pmod{g}$, $\alpha' \equiv \beta' \pmod{g}$, alors $\alpha\beta \equiv \alpha'\beta' \pmod{g}$.

Tous les éléments congrus à un d'entre eux forment un *complexe* (par exemple les éléments de g forment un complexe). Si l'on fait le produit de tous les éléments d'un complexe A par tous les éléments d'un autre complexe B, on n'obtiendra que les éléments d'un même complexe C, dit *produit* de A et de B. Les complexes forment alors, par rapport à cette opération, un groupe, dit *groupe quotient* de G et de g, qui est isomorphe mériédriquement à G, un élément de G correspondant au complexe qui contient cet élément.

Désignons ce nouveau groupe par g'; on écrit G : $g \simeq g'$ (1*). Si G est fini, l'ordre de G : g est le quotient des ordres de G et de g.

Supposons maintenant G fini, et prenons un élément et un seul dans chaque complexe; soient $\sigma_1, \sigma_2, \ldots, \sigma_u$ ces éléments; tout élément de G est le produit d'un élément de g et d'un des σ_i, et réciproquement tous ces produits donnent des éléments différents de G. On écrit

$$G = g\sigma_1 + g\sigma_2 + \ldots + g\sigma_u,$$

et l'on dit que l'on a décomposé G suivant g.

4. Un groupe est dit *abélien* si pour deux quelconques a et b de ses éléments, on a $ab = ba$. Presque tous les groupes que nous considérerons seront abéliens.

Tout sous-groupe g d'un groupe abélien G est invariant. La notion de congruence par rapport à g est alors bien simple : à deux éléments quelconques a et b correspond un élément x, dit quotient de a par b, tel que $ax = xa = b$. Deux éléments a et b sont alors

(1*) Le groupe quotient se désigne le plus souvent par G/g.

du même complexe si, et seulement si, le quotient de l'un par l'autre est dans g.

a étant un élément d'un groupe, les a^x (les puissances de a) forment un groupe abélien; m étant le plus petit entier positif tel que $a^m = e$, l'ordre de ce groupe est m. m est dit l'*ordre* de a; s'il n'y a pas de tel nombre m, l'ordre de a est dit infini.

Un groupe abélien est dit avoir une base composée des éléments σ_i ($i = 1, 2, \ldots, l$), $\sigma_1, \sigma_2, \ldots, \sigma_j$ étant d'ordres $m_1, m_2, \ldots, m_j$, les autres σ d'ordre infini, si les $\sigma_1^{x_1}, \sigma_2^{x_2}, \ldots, \sigma_l^{x_l}$ représentent tous les éléments du groupe une fois et une seule, les x_i parcourant tous les entiers positifs et négatifs avec la seule restriction

$$0 \leqq x_i < m_i \qquad (i = 1, 2, \ldots, j).$$

Si le groupe a une base d'un seul élément, il est dit *cyclique*.

Si $j = l$, le groupe est d'ordre fini, et a par ordre le produit des m_i.

On démontre que : *tout groupe abélien fini a une base telle que les ordres de tous les éléments de base soient des puissances de nombres premiers.*

5. Cherchons à attacher à tout élément d'un groupe abélien *fini* un nombre (réel ou complexe) non nul tel que si aux éléments a et b correspondent α et β, à ab corresponde le produit $\alpha\beta$. Ces nombres forment donc un groupe multiplicatif mériédriquement isomorphe au groupe donné. Un tel système de nombres est dit un système de *caractères* (ou, brièvement, un *caractère*) du groupe; le nombre attaché à a est dit le *caractère* de a dans ce système. On voit aisément que tout caractère est une racine de l'unité; et que le caractère de l'unité e du groupe est toujours 1.

On a un système particulier de caractères en faisant correspondre 1 à tous les éléments du groupe : c'est le *caractère principal*.

n étant l'ordre du groupe :

1° Il y a n systèmes différents de caractères;

2° La somme des caractères d'un même élément dans ces systèmes est 0 sauf pour l'élément unité où elle vaut n;

3° La somme des caractères d'un même système est 0 sauf pour le « caractère principal » où elle vaut n.

6. Soit G un groupe quelconque; le plus petit groupe g qui

contienne tous les éléments de forme $aba^{-1}b^{-1}$ est dit le *groupe des commutateurs* de g ($aba^{-1}b^{-1}$ est le *commutateur* de a et de b).

a. g est un sous-groupe invariant;

b. G : g est abélien;

c. Tout sous-groupe invariant g' tel que G : g' soit abélien contient g.

7. Étant donnés deux groupes g et g', un groupe G est dit *produit direct* de g et de g', quand il y a une correspondance biunivoque entre les éléments de G et les couples (a, b) d'éléments, dont le premier a est de g et le deuxième b de g'; de manière que si à A et B de G correspondent les couples (a, b) et (a', b'), à AB correspond $(ab, a'b')$. L'ordre de G est alors égal au produit des ordres de g et de g'.

Le produit direct de deux groupes abéliens est abélien.

II. — Corps algébriques.

Pour un exposé complet des paragraphes 2 et 3, on peut consulter Hasse [1, en particulier le deuxième volume], ou van der Waerden [2].

1. On appelle *nombre algébrique* tout nombre (réel ou imaginaire) qui est racine d'une équation algébrique à coefficients entiers. On démontre aisément que :

1° Toute racine d'une équation algébrique, dont les coefficients sont des nombres algébriques, est un nombre algébrique;

2° La somme, le produit, la différence, le quotient de deux nombres algébriques sont un nombre algébrique.

Un ensemble de nombres algébriques est dit former un *corps* lorsque le produit, le quotient, la somme et la différence de deux nombres de cet ensemble appartiennent à cet ensemble. C'est ainsi que les nombres rationnels forment un corps; tout autre corps contient celui-là.

On obtient des corps, d'une manière générale, en partant d'un corps k, et de nombres algébriques $\alpha_1, \alpha_2, \ldots$: l'ensemble des fonctions rationnelles de ces α_i à coefficients dans k forme un corps

que l'on désignera par $k(\alpha_1, \alpha_2, \ldots)$. On dit qu'on l'obtient en *adjoignant* les α_i à k.

Un corps sera désormais dit *réel*, si tous ses nombres sont réels; sans cela, il est dit *imaginaire*.

2. Un polynome dont les coefficients sont dans un corps k est dit *irréductible* dans ce corps, s'il n'est pas égal au produit de deux polynomes de degré plus petit à coefficients dans k. Toute la théorie ordinaire du p. g. c. d. des polynomes peut alors se faire en n'introduisant que des nombres de k. On démontre ainsi que :

a. Tout polynome est un produit de polynomes irréductibles et cette décomposition est unique (à des facteurs constants près);

b. Si deux polynomes irréductibles ont une racine commune, ils coïncident;

c. Si un polynome a une racine double, il n'est pas irréductible.

3. Si tous les éléments d'un corps k sont dans un corps K, k est dit un *sous-corps* de K, et K un *sur-corps* de k. On écrit $k \subset K$, $K \supset k$. Les éléments de K satisfont alors à des équations à coefficients dans k, irréductibles dans k. Nous supposerons que leur degré est borné, et nous appelerons le degré maximum n de ces équations le *degré de* K *par rapport* à k. Sans cela, nous dirons que ce degré est infini. Si, en particulier, k est le corps formé par les nombres rationnels, n est le *degré absolu* de K.

Nous désignerons désormais par kk' le plus petit corps contenant les corps k et k'.

On démontre que :

a. Si K est de dégré relatif fini n par rapport à k, il y a un nombre α de K satisfaisant à une équation de degré n irréductible dans k, tel que $K = k(\alpha)$;

b. Si $K_1 \subset K_2$, $K_2 \subset K_3$, le degré de K_3 par rapport à K_1 est le produit des degrés de K_3 par rapport à K_2, et de K_2 par rapport à K_1.

Désormais, quand nous parlerons d'un corps, il s'agira toujours d'un corps de degré fini par rapport au corps des nombres rationnels.

4. On peut considérer des corps dont les éléments ne sont pas des

nombres ordinaires, mais des objets quelconques, pourvu qu'on ait défini deux opérations ayant toutes les propriétés formelles de l'addition et de la multiplication. Toutes les propriétés précédentes subsistent pour ces corps « abstraits » (sauf $2c$ dans certains cas) (*voir* Steinitz [1]; ou, pour un exposé complet de toute l'algèbre des corps, l'excellent petit livre de Hasse [1], ou encore van der Waerden [2]). Nous en verrons des exemples plus loin.

III. — Théorie de Galois.

1. Soient k un corps, $K = k(\alpha)$ un sur-corps de degré relatif n par rapport à k. α satisfait (§ 2_{3a}) à une équation irréductible dans k de degré n. Soient $\alpha = \alpha^{(1)}, \alpha^{(2)}, \ldots, \alpha^{(n)}$ ses racines. Les corps $K = k(\alpha^{(1)}), k(\alpha^{(2)}), \ldots, k(\alpha^{(n)})$ sont dits les *conjugués* de K par rapport à k. Si ces n corps coïncident, K est dit *galoisien* par rapport à k.

Soit β un nombre de K; c'est une fonction rationnelle $R(\alpha)$ de α à coefficients dans k. Les $R(\alpha^{(i)})$ sont dits les conjugués de β par rapport à k. En particulier, les conjugués des nombres de k sont égaux entre eux.

Soit k' un corps intermédiaire : $k \subset k' \subset K$; quand β parcourt tous les nombres de k', les $R(\alpha^{(i)})$ forment un autre corps $k'^{(i)}$ qui est dit conjugué du premier par rapport à k.

$k(\alpha^{(i)})$, $R(\alpha^{(i)})$, $k'^{(i)}$ sont dits des *conjugués correspondants*. Les conjugués par rapport au corps des rationnels sont dits *conjugués absolus*.

Le produit des n conjugués de β par rapport à k est dit la *norme* de β (prise dans K par rapport à k). On la désigne par $N_{Kk}(\beta)$ [ou, quand aucune confusion n'est à craindre, par $N_k(\beta)$ ou $N(\beta)$]. Le produit des conjugués absolus est dit la *norme absolue*.

2. Supposons désormais K galoisien par rapport à k.

Un *automorphisme* T (nous dirons souvent une *substitution*) de K par rapport à k, est une transformation qui, à tout nombre α de K fait correspondre un nombre $T\alpha$ de K de manière que :

a. $T\alpha = T\beta$ entraîne $\alpha = \beta$;
b. $T\alpha = \alpha$ si α est dans k;
c. $T(\alpha + \beta) = T\alpha + T\beta$ et $T(\alpha\beta) = T\alpha . T\beta$.

On démontre que tout automorphisme T est tel que $T\beta = R(\alpha^{(i)})$ quand $\beta = R(\alpha)$. Une telle transformation étant évidemment un automorphisme, il y a n automorphismes (y compris l'automorphisme unité, tel que $T\alpha = \alpha$). Ils forment évidemment un groupe G dit « groupe de Galois » de K par rapport à k (l'automorphisme produit de T et T′ étant celui qu'on obtient en faisant d'abord la transformation T′, puis T).

Avec ces remarques, on démontre aisément que K est galoisien aussi par rapport à tout corps intermédiaire.

Si G est abélien (ou cyclique), K est dit *abélien* (ou *cyclique*) par rapport à k.

3. Le théorème fondamental de la théorie de Galois est le suivant :

a. A tout corps intermédiaire $k'(k \subset k' \subset K)$ *correspond un sous-groupe* g *de* G *formé des substitutions de* g *laissant invariants tous les nombres de* k'. g *est le groupe de Galois de* K *par rapport à* k' (*on dit que* k' *correspond à* g; *et réciproquement*);

b. Réciproquement à tout sous-groupe g *de* G *correspond un corps* k', *qui est formé des éléments invariants par les substitutions de* g;

c. σ *étant l'automorphisme qui transforme* α *en* $\alpha^{(i)}$, $\sigma k'$ *le conjugué correspondant de* k', *à* $\sigma k'$ *correspond le groupe* $\sigma g \sigma^{-1}$;

d. Pour que k' *soit galoisien par rapport à* k, *il faut et il suffit que* g' *soit un sous-groupe invariant; le groupe de Galois de* k' *par rapport à* k *est alors le groupe quotient de* G *par* g.

IV. — Entiers.

Pour le contenu des paragraphes 4 à 8, on peut consulter Hilbert [1; 1re partie] (exposé très dense et ardu); ou Hecke [1].

1. Un nombre α est un *entier algébrique* (ou, brièvement, un entier) s'il satisfait à une équation de la forme

$$x^n + a_1 x^{n-1} + \ldots + a_n = 0, \tag{1}$$

les a_i étant des entiers ordinaires, cette équation étant irréductible dans le corps des nombres rationnels.

En particulier, tout entier ordinaire est un entier algébrique.

On démontre que :

a. Toute racine d'une équation de forme (1) (irréductible ou non), où les a_i sont des entiers algébriques, est un entier algébrique;

b. La somme, la différence, le produit de deux entiers, est un entier;

c. Les seuls nombres rationnels qui soient des entiers algébriques sont les entiers ordinaires.

2. Soit un corps K de degré absolu n. Ses entiers forment un groupe abélien par rapport à l'addition. Ce groupe a une *base* de n éléments, $\alpha_1, \alpha_2, \ldots, \alpha_n$, de sorte que tout autre entier est de forme $x_1\alpha_1 + x_2\alpha_2 + \ldots + x_n\alpha_n$, les x_i étant des entiers ordinaires.

V. — Idéaux.

1. Étant donné un corps de nombres algébriques k, on appelle *idéal* de ce corps tout ensemble de nombres du corps tel que :

a. Si α fait partie de cet ensemble, il en est de même de $\lambda\alpha$ quel que soit l'entier λ;

b. Si β est un autre élément de cet ensemble, $\alpha + \beta$ en fait aussi partie;

c. Il y a un entier $\mu \neq 0$ tel que pour tout α de cet ensemble, $\mu\alpha$ soit entier.

Si tous les nombres de l'idéal sont entiers, l'idéal est dit *entier*.

2, Étant donné un ensemble quelconque de nombres du corps, α_1, $\alpha_2, \ldots$, l'ensemble des $\lambda_1\alpha_1 + \lambda_2\alpha_2 + \ldots$, les λ_i étant des entiers arbitraires du corps, forme un idéal appelé l'idéal *engendré* par les α_i; on le désigne par $(\alpha_1, \alpha_2, \ldots)$ (1*).

L'idéal (α) engendré par un seul nombre $\alpha \neq 0$ est dit *principal*.

3. On appelle *produit* de deux idéaux $\mathfrak{a}$ et $\mathfrak{b}$, l'idéal engendré par l'ensemble de nombres obtenus en multipliant un nombre de $\mathfrak{a}$ et un nombre de $\mathfrak{b}$.

(1*) A condition qu'il existe un entier $\mu \neq 0$ tel que les $\mu\alpha_i$ soient tous entiers.

Le produit des idéaux principaux (α) et (β) est $(\alpha\beta)$. Pour tout idéal $\mathfrak{a}$, on a $\mathfrak{a}(1) = \mathfrak{a}$: l'idéal (1) (formé de tous les entiers du corps) est dit l'*idéal unité*.

4. Dans le corps des nombres rationnels, tout idéal est principal : soit en effet $\mathfrak{a}$ un idéal, a le plus petit nombre positif de $\mathfrak{a}$, b un autre nombre de l'idéal; b est un multiple entier de a, car sans cela le reste de la division de b par a, de la forme $bx - a$ (x entier), serait un nombre de l'idéal plus petit que a.

Les idéaux et les nombres positifs se correspondent donc biunivoquement; et, dans ce cas, le théorème de la décomposition en facteurs premiers est vrai pour les idéaux.

5. Pour un corps quelconque, ce théorème n'est plus vrai pour les entiers, mais il le reste pour les idéaux. Appelons, en effet, idéal *premier* un idéal entier $\mathfrak{a}$ qui ne peut être mis sous la forme $\mathfrak{b}\mathfrak{c}$ où $\mathfrak{b}$ et $\mathfrak{c}$ sont entiers et différents de (1) :

a. Étant donnés deux idéaux $\mathfrak{a}$ et $\mathfrak{b}$, il y a un idéal $\mathfrak{c}$, tel que $\mathfrak{a}\mathfrak{c} = \mathfrak{b}$.

On écrit $\mathfrak{c} = \frac{\mathfrak{b}}{\mathfrak{a}}$. D'où la notion de quotient de deux idéaux. On désignera, en particulier, par $\mathfrak{a}^{-1}$ l'idéal $\frac{(1)}{\mathfrak{a}}$, par $\mathfrak{a}^{-n}$ la $n^{\text{ième}}$ puissance de $\mathfrak{a}^{-1}$. On convient que $\mathfrak{a}^0 = (1)$.

b. Tout idéal peut être mis d'une manière et d'une seule sous la forme : $\mathfrak{p}_1^{x_1}\mathfrak{p}_2^{x_2}\ldots\mathfrak{p}_n^{x_n}$, les $\mathfrak{p}_i$ étant des idéaux premiers, les x_i des entiers positifs ou négatifs. Pour que cet idéal soit entier, il faut et il suffit que les x_i soient positifs.

c. La condition nécessaire et suffisante pour que $\mathfrak{a}$ divise $\mathfrak{b}$ (c'est-à-dire pour qu'il y ait un idéal entier $\mathfrak{c}$ tel que $\mathfrak{a}\mathfrak{c} = \mathfrak{b}$) est que tout nombre de $\mathfrak{b}$ soit dans $\mathfrak{a}$.

En particulier, pour que $\mathfrak{a}$ divise un idéal principal (α), il faut et il suffit que α soit un nombre de $\mathfrak{a}$.

On peut alors développer la théorie du P. G. C. D. et du P. P. C. M. des idéaux entiers, comme pour les entiers rationnels; on dira, en particulier, que les idéaux entiers $\mathfrak{a}$ et $\mathfrak{b}$ sont premiers entre eux s'ils ne sont divisibles par aucun autre idéal entier que (1). On convient que tout idéal est premier à (1).

Il nous arrivera souvent de dire que le nombre α divise $\mathfrak{a}$, est premier à $\mathfrak{a}$, etc., au lieu de dire l'idéal (α) divise $\mathfrak{a}$, est premier à $\mathfrak{a}$, etc.

5. Les idéaux forment un groupe par rapport à la multiplication. Les idéaux principaux forment un sous-groupe.

Un complexe du groupe des idéaux par rapport à ce sous-groupe est dit une *classe* d'idéaux : une classe d'idéaux est donc formée de tous les idéaux dont le quotient par l'un d'entre eux est principal; les classes forment les éléments du groupe quotient de ces deux groupes, qui est dit *groupe des classes*.

On démontre que *le groupe des classes n'a qu'un nombre fini d'éléments*.

7. Soit $\mathfrak{a}$ un idéal d'un corps k; considérons un sur-corps K. Les nombres de $\mathfrak{a}$ engendrent dans K un idéal $\mathfrak{A}$: on démontre que tout nombre de k qui est dans $\mathfrak{A}$ est dans $\mathfrak{a}$. Si $\mathfrak{b}$ de k engendre $\mathfrak{B}$ dans K, $\mathfrak{ab}$ engendre $\mathfrak{AB}$.

Donc, quand on parle d'un idéal, il est inutile de fixer le corps dans lequel on le considère : on considérera comme identiques les idéaux $\mathfrak{a}$ et $\mathfrak{A}$. Il faut pourtant remarquer qu'un idéal n'est pas représenté dans n'importe quel corps : il y a des idéaux de K, qui ne sont identiques à aucun des idéaux de k.

Si deux idéaux sont premiers entre eux dans un corps, ils le sont dans tout autre corps.

8. Soit $\mathfrak{A}$ un idéal de K; les nombres de $\mathfrak{A}$ situés dans k forment un idéal $\mathfrak{a}$, qui peut être différent de $\mathfrak{A}$.

En tout cas $\mathfrak{A}$ divise $\mathfrak{a}$. Considérons tous les conjugués de $\mathfrak{A}$ (obtenus en remplaçant chaque nombre de $\mathfrak{A}$ par un conjugué correspondant par rapport à k) : tous ces idéaux divisent $\mathfrak{a}$. On démontre sans peine que leur produit est un idéal $\mathfrak{b}$ du corps k, qui est dit la *norme* de $\mathfrak{A}$ prise dans K par rapport à k; on écrit $\mathfrak{b} = N_{Kk}(\mathfrak{A})$ ou, si aucune confusion n'est à craindre, $N_k(\mathfrak{A})$ ou $N(\mathfrak{A})$. La norme d'un idéal par rapport au corps des rationnels, est dite la *norme absolue* de cet idéal. Si $\mathfrak{A}$ est principal : $\mathfrak{A} = (\alpha)$, on a $N_{Kk}(\mathfrak{A}) = \left(N_{Kk}(\alpha)\right)$.

b. Si $\mathfrak{A}$ est premier, on démontre sans peine que $\mathfrak{a}$ est aussi pre-

mier et que $N_{Kk}(\mathfrak{A})$ est une puissance $\mathfrak{a}^f$ de $\mathfrak{a}$. f est dit le *degré* de $\mathfrak{A}$ par rapport à k.

c. Si $\bar{k}$ est un sous-corps de k, et si $\mathfrak{a}$ a le degré f' par rapport à $\bar{k}$, $\mathfrak{A}$ a le degré ff' par rapport à $\bar{k}$: les degrés se multiplient.

d. Prenons un idéal premier $\mathfrak{p}$ de k, et considérons-le dans K; dans K, il n'est pas forcément premier; on aura $\mathfrak{p} = \mathfrak{P}_1^{e_1}, \mathfrak{P}_2^{e_2}, \ldots, \mathfrak{P}_g^{e_g}$, les $\mathfrak{P}_i$ étant des idéaux premiers de K. Les nombres de $\mathfrak{P}_i$ qui sont dans k forment $\mathfrak{p}$. En prenant les normes des deux membres, on voit que, f_i désignant le degré de $\mathfrak{P}_i$ par rapport à k, $e_1 f_1 + e_2 f_2 + \ldots + e_g f_g$ est égal au degré relatif de K par rapport à k.

Si tous les e_i sont égaux à 1, on dit que $\mathfrak{p}$ est *non-ramifié* dans K; sans cela qu'il est *ramifié*.

VI. — Unités.

1. Un nombre ε est une *unité* si ε et $\frac{1}{\varepsilon}$ sont entiers.

2. Pour qu'un idéal principal (α) soit l'idéal unité, il faut et il suffit que α soit une unité.

Donc pour que deux idéaux principaux (α) et (β) soient identiques, il faut et il suffit que $\frac{\alpha}{\beta}$ soit une unité.

3. Les unités forment un groupe abélien, sous-groupe du groupe abélien multiplicatif des nombres du corps différents de 0.

On voit que le groupe quotient de ces deux groupes est isomorphe au groupe des idéaux principaux.

4. Dirichlet (Hilbert [1; Livre 1, Chap. 6]) (*cf.* aussi Van der Waerden [1]) a démontré que le groupe des unités avait une base bien définie :

Toute unité est représentable d'une manière bien déterminée sous la forme : $\zeta^y \varepsilon_1^{x_1} \varepsilon_2^{x_2} \ldots \varepsilon_r^{x_r}$, ζ *étant une racine* $m^{\text{ième}}$ *primitive de l'unité* (*on peut avoir* $m = 1$), *les* y *et les* x_i *sont des entiers* $\geqq 0$ *quelconques, avec la seule restriction* $0 \leqq y < m$.

Si, parmi les corps k *et ses conjugués,* r_1 *sont réels, et* $2r_2$ *imaginaires, on a* $r = r_1 + r_2 - 1$.

VII. — Congruences.

Pour ce paragraphe, *voir* particulièrement Hasse [3, p. 59-64].

1. Soit $\mathfrak{a}$ un idéal entier du corps k. On définit habituellement les congruences par rapport à $\mathfrak{a}$ de la façon suivante : on considère tous les entiers du corps, qui forment un groupe par rapport à l'addition; puis le sous-groupe de tous ceux de ces entiers qui sont situés dans $\mathfrak{a}$.

Un complexe du premier groupe par rapport à ce sous-groupe est dit une classe de congruence (mod $\mathfrak{a}$); deux entiers α et β sont dits congrus entre eux (mod $\mathfrak{a}$) [et l'on écrit alors $\alpha \equiv \beta \pmod{\mathfrak{a}}$] s'ils sont dans la même classe de congruence (mod $\mathfrak{a}$); il faut et il suffit pour cela que $\alpha - \beta$ soit dans $\mathfrak{a}$. Les classes de congruence (mod $\mathfrak{a}$) sont les éléments du groupe quotient de ces deux groupes. On démontre que son ordre est égal à la norme absolue de $\mathfrak{a}$.

Tous les nombres congrus à l'un d'entre eux forment une classe de congruence. D'après leur définition même, ces classes peuvent s'additionner; mais on peut aussi les multiplier, car les produits de tous les nombres d'une classe par tous les nombres d'une autre classe sont tous dans une même classe dite *produit* des deux premières.

Mais si l'on veut que ces classes forment un groupe par rapport à la multiplication, il faut se limiter à celles qui contiennent des nombres premiers à $\mathfrak{a}$. Car on démontre que ce n'est que si α est premier à $\mathfrak{a}$ que l'on peut trouver un x tel que $\alpha x \equiv 1 \pmod{\mathfrak{a}}$. Comme seuls nous intéresseront désormais ces groupes multiplicatifs, il est préférable de les introduire directement.

2. Un idéal sera désormais dit *entier pour* $\mathfrak{a}$, si on peut le mettre sous la forme $\frac{\mathfrak{b}}{\mathfrak{c}}$, $\mathfrak{b}$ étant entier, $\mathfrak{c}$ entier et premier à $\mathfrak{a}$. Il sera dit *premier à* $\mathfrak{a}$ si de plus $\mathfrak{b}$ est premier à $\mathfrak{a}$.

Les nombres premiers à $\mathfrak{a}$ forment un groupe $g_{\mathfrak{a}}$ par rapport à la multiplication; les idéaux premiers à $\mathfrak{a}$ forment de même un groupe $A_{\mathfrak{a}}$ par rapport à la multiplication.

Les nombres α de $g_{\mathfrak{a}}$ tels que $\alpha - 1$ soit de numérateur divisible [1]

---

[1] Nous avons dit plus haut (§ 5_5) que dans de telles expressions, on parlait du nombre, au lieu de l'idéal principal engendré par le nombre.

par $\mathfrak{a}$ forment un groupe $h_{\mathfrak{a}}$ par rapport à la multiplication [cela résulte de l'identité $\alpha\beta - 1 = (\alpha - 1)(\beta - 1) + (\alpha - 1) + (\beta - 1)$].

Un complexe de $g_{\mathfrak{a}}$ par rapport à $h_{\mathfrak{a}}$ sera dit une *classe de congruence* (mod $\mathfrak{a}$). On démontre en effet que pour que deux nombres entiers et premiers à $\mathfrak{a}$ soient dans la même classe au nouveau sens, il faut et il suffit qu'il en soit ainsi avec l'ancien sens. Deux nombres α et β seront dits congrus entre eux (mod $\mathfrak{a}$) [et l'on écrira encore $\alpha \equiv \beta \pmod{\mathfrak{a}}$] s'ils sont de la même classe de congruence. Pour qu'il en soit ainsi, il faut et il suffit que $\frac{\alpha}{\beta} - 1$ soit de numérateur divisible par $\mathfrak{a}$. Les classes de congruence (mod $\mathfrak{a}$) sont par définition les éléments du groupe quotient.

Si $\mathfrak{a}$ est premier, ce groupe est cyclique d'ordre $N\mathfrak{a} - 1$ ($N\mathfrak{a}$ étant la norme absolue de $\mathfrak{a}$).

Si $\mathfrak{a}$ et $\mathfrak{b}$ sont premiers entre eux, $h_{\mathfrak{ab}}$ est composé des éléments communs à $h_{\mathfrak{a}}$ et à $h_{\mathfrak{b}}$; $\frac{g_{\mathfrak{ab}}}{h_{\mathfrak{ab}}}$ est isomorphe au produit direct de $\frac{g_{\mathfrak{a}}}{h_{\mathfrak{a}}}$ et de $\frac{g_{\mathfrak{b}}}{h_{\mathfrak{b}}}$.

Si $\mathfrak{a} = (1)$, on convient que $A_{\mathfrak{a}}$ est le groupe de tous les idéaux, $g_{\mathfrak{a}} = h_{\mathfrak{a}}$ celui de tous les nombres différents de o.

3. Hasse (*loc. cit.*) a introduit des éléments fictifs, les *idéaux infinis*, qui nous seront d'une grande utilité. Ce sont des idéaux fictifs que l'on fait correspondre à certains groupes de nombres, de la même manière que $\mathfrak{a}$ correspond au groupe $h_{\mathfrak{a}}$.

Considérons parmi tous les corps conjugués de k un corps réel (s'il y en a). Les nombres α de k tels que leur conjugué correspondant soit positif, forment un groupe que l'on désignera par $h_{\tilde{\mathfrak{p}}_1}$ et que l'on fera correspondre à l'idéal infini $\tilde{\mathfrak{p}}_1$. Il y a autant d'idéaux à l'infini que de conjugués réels de k.

Soient $\tilde{\mathfrak{p}}_1, \tilde{\mathfrak{p}}_2, \ldots, \tilde{\mathfrak{p}}_s$ ces idéaux.

On introduira des idéaux généralisés $\tilde{\mathfrak{a}}$ (qui sont de simples symboles), produit d'un idéal ordinaire $\mathfrak{a}$, et d'un certain nombre d'idéaux $\tilde{\mathfrak{p}}_i$ différents. Par convention les nombres et les idéaux premiers à $\tilde{\mathfrak{a}}$, sont les mêmes que ceux qui sont premiers à $\mathfrak{a}$ [si $\mathfrak{a} = (1)$, tous les nombres $\neq$ o, et tous les idéaux]; donc l'on pose $A_{\mathfrak{a}} = A_{\tilde{\mathfrak{a}}}$,

$g_{\mathfrak{a}} = g_{\tilde{\mathfrak{a}}}$. $h_{\tilde{\mathfrak{a}}}$ est formé par convention des nombres communs à $h_{\mathfrak{a}}$ et aux $h_{\tilde{\mathfrak{p}}_i}$, pour tous les $\tilde{\mathfrak{p}}_i$ figurant dans $\tilde{\mathfrak{a}}$. Les éléments du groupe quotient $g_{\tilde{\mathfrak{a}}} : h_{\tilde{\mathfrak{a}}}$ sont encore dits les classes de congruence $(\bmod \tilde{\mathfrak{a}})$; deux nombres de la même classe sont encore dits congrus $(\bmod \tilde{\mathfrak{a}})$, et l'on écrit $\alpha \equiv \beta \ (\bmod \tilde{\mathfrak{a}})$.

En particulier $h_{\tilde{\mathfrak{p}}_1 \tilde{\mathfrak{p}}_2 \ldots \tilde{\mathfrak{p}}_s}$ est le groupe des nombres dont les conjugués correspondants aux conjugués réels de k sont positifs. Un tel nombre est dit *totalement positif*.

Nous conviendrons que $\tilde{\mathfrak{p}}_i^x$ (qui jusqu'ici n'a pas de sens) est identique à $\tilde{\mathfrak{p}}_i$.

Nous dirons souvent dans la suite idéaux *finis* au lieu d'idéaux ordinaires (par opposition aux idéaux *infinis*).

Désormais, quand nous voudrons indiquer qu'un idéal peut être quelconque (ordinaire ou généralisé), nous le ferons surmonter du signe $\sim$. A défaut de ce signe, ou de l'indication explicite du contraire, un idéal dans ce qui suit est ordinaire.

4. Soit $G_{\tilde{\mathfrak{a}}}$ le groupe des idéaux (α), α étant dans $\mathfrak{g}_{\tilde{\mathfrak{a}}}$. Les idéaux (α) tels que α soit dans $h_{\tilde{\mathfrak{a}}}$ forment un groupe $H_{\tilde{\mathfrak{a}}}$, sous-groupe de $G_{\tilde{\mathfrak{a}}}$, qui est dit le *rayon* mod $\tilde{\mathfrak{a}}$.

Le groupe quotient $G_{\tilde{\mathfrak{a}}} : H_{\tilde{\mathfrak{a}}}$ n'est pas identique au groupe $g_{\tilde{\mathfrak{a}}} : h_{\tilde{\mathfrak{a}}}$; en effet, ε étant une unité telle que $\varepsilon \not\equiv 1 \ (\bmod \tilde{\mathfrak{a}})$, α et $\varepsilon\alpha$ ne sont pas congrus suivant $h_{\tilde{\mathfrak{a}}}$ et cependant $(\alpha) = (\varepsilon\alpha)$. Par contre, si on considère le groupe $k_{\tilde{\mathfrak{a}}}$ des nombres de $g_{\tilde{\mathfrak{a}}}$ qui sont congrus $(\bmod \tilde{\mathfrak{a}})$ à des unités, on a $G_{\tilde{\mathfrak{a}}} : H_{\tilde{\mathfrak{a}}} = g_{\tilde{\mathfrak{a}}} : k_{\tilde{\mathfrak{a}}}$.

Nous appellerons désormais *groupes d'idéaux*, seulement les groupes qui, pour un $\tilde{\mathfrak{a}}$ convenablement choisi, sont identiques à un sous-groupe $K_{\tilde{\mathfrak{a}}}$ de $A_{\tilde{\mathfrak{a}}}$ qui contient $H_{\tilde{\mathfrak{a}}}$. $K_{\tilde{\mathfrak{a}}}$ sera dit *défini* mod $\tilde{\mathfrak{a}}$.

Nous mettons dans la même classe (*classes suivant* $K_{\tilde{\mathfrak{a}}}$) deux idéaux dont le quotient est dans $K_{\tilde{\mathfrak{a}}}$; les classes sont identiques aux complexes de $A_{\tilde{\mathfrak{a}}}$ suivant $K_{\tilde{\mathfrak{a}}}$; ce sont les éléments du groupe quotient $A_{\tilde{\mathfrak{a}}} : K_{\tilde{\mathfrak{a}}}$. L'ordre de ce groupe est fini et est dit *l'indice* de $K_{\tilde{\mathfrak{a}}}$.

Cette notion de classe généralise celle déjà considérée et il importe de bien se rendre compte de la manière dont elle est obtenue. Si $\tilde{\mathfrak{a}} = (1)$, $H_{\tilde{\mathfrak{a}}}$ est composé des idéaux principaux, $A_{\tilde{\mathfrak{a}}}$ de tous les idéaux; si $K_{\tilde{\mathfrak{a}}} = H_{\tilde{\mathfrak{a}}}$ on a la notion de classe du paragraphe 6_6 (nous appellerons ces classes, *classes au sens ordinaire*). Si nous rem-

UNIVERSITÉ DE GRENOBLE I
LABORATOIRE
DE MATHÉMATIQUES PURES
INSTITUT FOURIER

plaçons (1) par $\tilde{\mathfrak{a}}$, il y a moins d'idéaux dans $H_{\tilde{\mathfrak{a}}}$ que dans $H_{(1)}$; si $K_{\tilde{\mathfrak{a}}} = H_{\tilde{\mathfrak{a}}}$, la notion de classe est devenue plus « fine » (le fait qu'on ne considère que les idéaux premiers à $\tilde{\mathfrak{a}}$ est sans importance essentielle). Si $K_{\tilde{\mathfrak{a}}}$ est différent de $H_{\tilde{\mathfrak{a}}}$, une classe suivant $K_{\tilde{\mathfrak{a}}}$ est formée de la réunion de plusieurs classes suivant $H_{\tilde{\mathfrak{a}}}$: la notion de classe est au contraire devenue plus « grossière ».

Prenons encore pour $\tilde{\mathfrak{a}}$ le produit de tous les idéaux à l'infini. $H_{\tilde{\mathfrak{a}}}$ se compose de tous les idéaux (α) tels que α soit totalement positif. Les classes suivant $H_{\tilde{\mathfrak{a}}}$ sont dites les *classes au sens restreint*.

5. Considérons deux groupes d'idéaux $K_{\tilde{\mathfrak{a}}}$ et $K_{\tilde{\mathfrak{b}}}$ définis $(\text{mod } \tilde{\mathfrak{a}})$ et $(\text{mod } \tilde{\mathfrak{b}})$. On dira que ces groupes sont égaux si les idéaux premiers à $\tilde{\mathfrak{a}}$ et à $\tilde{\mathfrak{b}}$ qu'ils contiennent sont les mêmes.

On dira que $K_{\tilde{\mathfrak{a}}}$ est plus petit que $K_{\tilde{\mathfrak{b}}}$, ou $K_{\tilde{\mathfrak{b}}}$ plus grand que $K_{\tilde{\mathfrak{a}}}$ et l'on écrira $K_{\tilde{\mathfrak{a}}} \subset K_{\tilde{\mathfrak{b}}}$, $K_{\tilde{\mathfrak{b}}} \supset K_{\tilde{\mathfrak{a}}}$, si tous les idéaux de $K_{\tilde{\mathfrak{a}}}$ premiers à $\tilde{\mathfrak{a}}$ et à $\tilde{\mathfrak{b}}$ sont dans $K_{\tilde{\mathfrak{b}}}$, sans que la réciproque soit vraie. On voit aisément que ces notions possèdent les propriétés habituelles de l'égalité et de l'inégalité.

Si $K_{\tilde{\mathfrak{a}}}$ et $K_{\tilde{\mathfrak{b}}}$ sont égaux, les groupes des classes suivant $K_{\tilde{\mathfrak{a}}}$ et $K_{\tilde{\mathfrak{b}}}$ sont isomorphes.

On peut toujours définir suivant différents modules $\tilde{\mathfrak{m}}$, des groupes d'idéaux égaux à $K_{\tilde{\mathfrak{a}}}$: savoir les modules $\tilde{\mathfrak{m}}$ tels que les idéaux de $H_{\tilde{\mathfrak{m}}}$ premiers à $\tilde{\mathfrak{a}}$ soient dans $K_{\tilde{\mathfrak{a}}}$; il en sera ainsi par exemple pour tous les $\tilde{\mathfrak{m}}$ multiples de $\tilde{\mathfrak{a}}$. Tous ces modules sont des multiples d'un d'entre eux, $\tilde{\mathfrak{f}}$, dit le *conducteur* de $K_{\tilde{\mathfrak{a}}}$.

6. Considérons un système de caractères du groupe des classes suivant $K_{\tilde{\mathfrak{f}}}$, $K_{\tilde{\mathfrak{f}}}$ étant un groupe d'idéaux de conducteur $\tilde{\mathfrak{f}}$. Celles de ces classes qui ont un caractère égal à 1 dans ce système forment un groupe d'idéaux K'. Le conducteur $\tilde{\mathfrak{f}}'$ de K' est un diviseur de $\tilde{\mathfrak{f}}$, dit *conducteur du caractère*.

Si $\tilde{\mathfrak{f}}' = \tilde{\mathfrak{f}}$, on dit que le caractère est un *caractère propre*.

VIII. — Différente et discriminant.

1. Soient k un corps, K un sur-corps, $\alpha_1, \alpha_2, \ldots, \alpha_N$ une base des entiers de K (§ 4_2); $\alpha_1^{(i)}, \alpha_2^{(i)}, \ldots, \alpha_N^{(i)}$ un système de conjugués corres-

pondants des $\alpha_j (i = 1, 2, \ldots, N; \alpha_j^{(1)} = \alpha_j)$. Soit b_i l'idéal P. G. C. D. des $\alpha_j^{(i)} - \alpha_j (j = 1, 2, \ldots, N)$; soit δ le produit $b_2 b_3 \ldots b_n$; $\Delta = N_{Kk}(\delta)$ la norme de δ dans k : Δ est un idéal de k ; δ un idéal de K.

δ et Δ sont dits respectivement la *différente* et le *discriminant* de K par rapport à k.

2. *a. Pour qu'un idéal premier de k divise Δ, il faut et il suffit qu'il soit ramifié.*

Donc *il n'y a qu'un nombre fini d'idéaux premiers ramifiés.* Si $\Delta = (1)$, il n'y en a pas.

b. Soient $\overline{K}$ un sur-corps de K; $\overline{\delta}$ la différence de $\overline{K}$ par rapport à k; $\overline{\overline{\delta}}$ celle de $\overline{K}$ par rapport à K; on a $\overline{\delta} = \overline{\overline{\delta}}\,\delta$.

c. Si k est le corps des rationnels, Δ est engendré par le carré du déterminant des $\alpha_j^{(i)}$ (généralisation dans *Hilbert* [1 ; Chap. V]).

d. Si k est le corps des rationnels, $\Delta \neq (1)$, donc il y a toujours des idéaux premiers ramifiés. Le fait que ceci n'est pas général, est d'une importance capitale dans la suite.

3. Soient k' un conjugué réel de k, $\tilde{\mathfrak{p}}$ l'idéal infini correspondant; $K'^{(1)}, K'^{(2)}, \ldots, K'^{(n)}$ ceux des conjugués de K tel que le conjugué correspondant de k soit k'.

On dit que $\tilde{\mathfrak{p}}$ est *ramifié* si l'un de ces corps est imaginaire. Si K est galoisien par rapport à k, tous ces corps sont imaginaires, si l'un d'entre eux l'est.

Nous conviendrons que $\tilde{\mathfrak{p}}$ est « égal » au produit des idéaux infinis de K correspondants à ceux des $K'^{(i)}$ qui sont réels.

Le produit du discriminant par les idéaux infinis ramifiés est un idéal généralisé, dit *discriminant généralisé.*

Si ce discriminant est égal à (1), nous dirons que K est *non ramifié* par rapport à k : c'est la condition nécessaire et suffisante pour qu'aucun idéal premier (fini ou infini) ne soit ramifié.

IX. — Groupes de décomposition, d'inertie et de ramification [1].

1. Soit un corps K galoisien par rapport à k, de groupe de Galois G, de degré relatif n; k sera désormais le « corps de base »,

[1] Pour cette théorie, voir Hilbert [1, chap. X], Hasse [3, p. 69] et Chevalley [4].

et il est bien entendu que toutes les notions que nous allons définir ne le sont que « par rapport à k ».

On dit que l'idéal $\mathfrak{a}'$ est conjugué de l'idéal $\mathfrak{a}$, si $\mathfrak{a}'$ est formé par les transformés de tous les nombres de $\mathfrak{a}$ par un même automorphisme σ de K par rapport à k; on écrit $\mathfrak{a}' = \sigma\mathfrak{a}$.

Soit $\mathfrak{p}$ un idéal premier ordinaire de k. Comme au paragraphe 5_{8d}, décomposons-le dans K en un produit d'idéaux premiers, ces idéaux sont conjugués entre eux; on en déduit sans peine que :

$$\mathfrak{p} = (\mathfrak{P}_1 \mathfrak{P}_2 \ldots \mathfrak{P}_g)^e,$$

les $\mathfrak{P}_i$ étant des idéaux premiers de K. Soit f le degré des $\mathfrak{P}_i$ par rapport à k; on a (§ 5_{8d})

$$efg = n.$$

Les substitutions de G qui laissent $\mathfrak{P}_1$ invariant forment un groupe g_0 dit *groupe de décomposition* de $\mathfrak{P}_1$. Toute subtitution σ de g_0 est donc telle que $\alpha \equiv 0 \pmod{\mathfrak{P}_1}$ entraîne $\sigma\alpha \equiv 0 \pmod{\mathfrak{P}_1}$, donc que $\alpha \equiv \beta \pmod{\mathfrak{P}_1}$ entraîne $\sigma\alpha \equiv \sigma\beta \pmod{\mathfrak{P}_1}$ (α et β entiers); donc σ permute les classes de congruence suivant $\mathfrak{P}_1$.

Les substitutions σ de G qui laissent ces classes invariantes, donc telles que $\alpha \equiv \sigma\alpha \pmod{\mathfrak{P}_1}$ pour tout α entier, forment un groupe g_2 dit *groupe d'inertie* de $\mathfrak{P}_1$.

D'une manière générale, les substitutions σ telles que $\alpha \equiv \sigma\alpha \pmod{\mathfrak{P}_1^r}$ forment un groupe g_r dit $(r-1)^{\text{ième}}$ *groupe de ramification*.

2. On démontre que :

a. Si $\mathfrak{P}_i = \tau\mathfrak{P}_1$, τ étant un élément de G, le groupe de décomposition de $\mathfrak{P}_i$ est $\tau g_0 \tau^{-1}$, le groupe d'inertie est $\tau g_1 \tau^{-1}$, le $(r-1)^{\text{ième}}$ groupe de ramification est $\tau g_r \tau^{-1}$.

b. Le groupe d'inertie est d'ordre e; pour qu'il ait des éléments différents de l'unité, il faut donc et il suffit que $\mathfrak{p}$ soit ramifié dans K.

c. C'est un *sous-groupe invariant* de g_0; le groupe quotient est *cyclique* d'ordre f.

d. Supposons pour simplifier $e = 1$; g_1 se réduit à l'élément unité. Alors il y a une substitution σ de g_0 tel que $\sigma\alpha \equiv \alpha^{N\mathfrak{p}} \pmod{\mathfrak{P}_1}$, $N\mathfrak{p}$ étant la norme absolue de $\mathfrak{p}$. g_0 est formé des puissances successives de σ. On écrit $\left[\frac{K \mid k}{\mathfrak{P}_1}\right] = \sigma$ (ou bien, quand aucune confusion n'est à

craindre $\left[\frac{K}{\mathfrak{P}_1}\right] = \sigma$); c'est ce qu'on appelle la « substitution de *Frobenius* de $\mathfrak{P}_1$.

e. Si $\mathfrak{P}_i = \tau\mathfrak{P}_1$, τ étant un élément de G, on a

$$\left[\frac{K}{\mathfrak{P}_i}\right] = \tau\sigma\tau^{-1}.$$

Supposons en particulier G abélien; alors on aura $\left[\frac{K}{\mathfrak{P}_i}\right] = \sigma$ pour tout i; donc

$$\sigma\alpha \equiv \alpha^{N\mathfrak{p}} \pmod{\mathfrak{P}_i},$$

pour tout i; donc $\mathfrak{p}$ étant le produit des $\mathfrak{P}_i$:

$$\sigma\alpha \equiv \alpha^{N\mathfrak{p}} \pmod{\mathfrak{p}}.$$

σ ne dépend donc que de $\mathfrak{p}$; on écrit

$$\left(\frac{K \mid k}{\mathfrak{p}}\right) = \sigma \qquad \text{ou} \qquad \left(\frac{K}{\mathfrak{p}}\right) = \sigma.$$

3. *a*. Soit $e = p^{r_1}q$ (p étant le nombre premier divisible par $\mathfrak{p}$, q premier à p). q divise $N\mathfrak{p} - 1$; g_2 est un sous-groupe invariant de g_1 de degré p^{r_1}; le groupe quotient est cyclique.

b. En général, g_r est un sous-groupe invariant de g_{r-1} (et même de g_0); le groupe quotient de g_r et de g_{r-1} est abélien. Pour d'autres propriétés de ces groupes, *voir* Hasse (2, p. 69 et suiv., [26]), Speiser [2].

c. p^{r_i-1} étant de l'ordre de g_i ($i \geqq 2$), la plus haute puissance de $\mathfrak{P}$ par laquelle est divisible la différente a pour exposant

$$(e-1) + (p^{r_1}-1) + (p^{r_2}-1) + \ldots.$$

d. Soit K′ un corps intermédiaire ($k \subset K' \subset K$) correspondant au sous-groupe g de G.

Les groupes de décomposition, d'inertie, de ramification de $\mathfrak{P}_1$ par rapport à K′, sont formés par les éléments communs à g et aux groupes correspondants de $\mathfrak{P}_1$ par rapport à k.

$\left[\frac{K \mid K'}{\mathfrak{P}_1}\right]$ est la plus petite puissance de $\left[\frac{K \mid k}{\mathfrak{P}_1}\right]$ qui soit dans g. (Artin [6], Hasse [4, p. 8]).

d. Si K′ est galoisien par rapport à k, soit $\mathfrak{P}'$ l'idéal premier de K′ qui est divisible par $\mathfrak{P}_1$; on a vu (§ 1_3) que G : g est isomorphe au

groupe de K′ par rapport à K. Les éléments de ce groupe qui correspondent dans cet isomorphisme aux éléments des groupes de décomposition, d'inertie de $\mathfrak{P}_1$ par rapport à k, à $\left[\frac{K \mid k}{\mathfrak{p}_1}\right]$, forment respectivement les groupes de décomposition, d'inertie de $\mathfrak{P}'$ par rapport à k, ou $\left[\frac{K' \mid k}{\mathfrak{p}'}\right]$. Pour les groupes de ramification, la règle est plus compliquée (Herbrand [1], Hasse [26]).

X. — La fonction $\zeta(s)$ et ses généralisations.

On sait le rôle important joué dans la théorie des nombres premiers par la fonction

$$\zeta(s) = \prod \frac{1}{1-p^{-s}} = \sum \frac{1}{n^s},$$

le produit étant étendu à tous les nombres premiers p, la somme à tous les entiers rationnels n. On peut introduire une telle fonction pour tout corps algébrique k; on pose

$$\zeta_k(s) = \prod \frac{1}{1-(N\mathfrak{p})^{-s}} = \sum \frac{1}{(N\mathfrak{a})^s},$$

$N\mathfrak{a}$ désignant la norme absolue de l'idéal $\mathfrak{a}$, le produit étant étendu à tous les idéaux premiers, la somme à tous les idéaux entiers; un calcul aisé montre l'identité des deux dernières expressions. On peut encore généraliser cette fonction. Considérons une division des idéaux en classes suivant un groupe d'idéaux H_0 de conducteur $\tilde{\mathfrak{f}}$ (§ 7_4). Soit χ un système de caractères de ce groupe; nous appelerons $\chi(\mathfrak{a})$ pour un idéal $\mathfrak{a}$ premier à $\tilde{\mathfrak{f}}$, le caractère de la classe de $\mathfrak{a}$. On pose de même

$$L_k(s; \chi) = \prod \frac{1}{1-\chi(\mathfrak{p})(N\mathfrak{p})^{-s}} = \sum \frac{\chi(\mathfrak{a})}{(N\mathfrak{a})^{-s}},$$

le produit étant étendu à tous les idéaux premiers $\mathfrak{p}$, premiers à $\tilde{\mathfrak{f}}$; la somme à tous les idéaux premiers à $\tilde{\mathfrak{f}}$. Si χ est caractère principal, $L_k(s, \chi)$ ne diffère de $\zeta_k(s)$ que par un nombre fini de facteurs, correspondant aux idéaux premiers de $\tilde{\mathfrak{f}}$; si donc de plus $\tilde{\mathfrak{f}} = (1)$ (division en classes ordinaires), $L_k(s, \chi) = \zeta_k(s)$. On démontre que :

1° *Si χ n'est pas le caractère principal, la représentation*

de $L_k(s, \chi)$ *sous forme de série converge pour* $\mathfrak{R}(s) > \theta$ [$\theta < 1$; $\mathfrak{R}(s)$ désigne la partie réelle de s].

2° *Si* χ *est le caractère principal, les deux représentations de* $L_k(s, \chi)$ *convergent pour* $\mathfrak{R}(s) > 1$; *la limite de* $(s-1)L_k(s, \chi)$ *quand* s *tend vers* 1 *est finie; elle peut se calculer à partir du nombre de classes du corps et de ses unités.*

3° *Si* χ *est un caractère propre non principal* [on remarquera que tout $L_k(s, \chi)$ ne diffère que par un nombre fini de facteurs d'une telle fonction correspondant à un caractère propre], $L_k(s, \chi)$ *est une fonction entière;* $\zeta_k(s)$ *est méromorphe, et a un seul pôle simple en* $s = 1$.

4° $\frac{L(s, \chi)}{L(1-s, \bar{\chi})}$ ($\bar{\chi}$ *étant le caractère conjugué de* χ), *et* $\frac{\zeta_k(s)}{\zeta_k(1-s)}$ *sont égaux à des expressions élémentaires (formées d'une manière simple avec la fonction* Γ *et les fonctions* sin *et* cos) (Hecke [4], Siegel [1], *cf.* aussi Hasse [2, p. 35]).

Les deux premiers énoncés qui seront seuls employés dans la suite se démontrent par des calculs élémentaires (Weber [3]), les deux derniers nécessitent au contraire des moyens analytiques très puissants.

Un calcul simple montre que

$$\log L_k(s, \chi) = \sum \frac{\chi(\mathfrak{p})}{(N\mathfrak{p})^s} + g(s, \chi), \tag{1}$$

g étant une fonction définie et continue pour $\mathfrak{R}(s) > \frac{1}{2}$, la somme étant étendue aux idéaux premiers non diviseurs de $\mathfrak{f}$.

Soient H une de nos classes d'idéaux, χ_0 son caractère, h le nombre de ces classes; on aura, d'après I_5

$$\sum \chi_0^{-1} \log L_k(s, \chi) = h \sum \frac{1}{(N\mathfrak{p})^{-s}} + \sum \chi_0 g(s, \chi),$$

la somme étendue aux idéaux premiers de H. Faisons tendre s vers 1; $\log L_k(s, \chi)$ pour le caractère principal tend vers ∞; $g(s, \chi)$ est continue; donc :

5° *Si l'on peut démontrer que* $L_k(1, \chi) \neq 0$ *pour un caractère* χ *non principal, on en déduira qu'il y a une infinité d'idéaux premiers dans toute classe.*

Cette non annulation sera démontrée plus loin. Le théorème ci-dessus fournit alors une *vaste généralisation du théorème de Dirichlet sur la progression arithmétique.*

Les méthodes de Landau [1] permettent alors de démontrer que

$$\mathfrak{N}(x) = \frac{1}{k}\int^{x} \frac{du}{\log u} + O(xe^{-\alpha\sqrt{\log x}}),$$

$\mathfrak{N}(x)$ étant le nombre des idéaux premiers d'une classe de norme absolue inférieure à x; α une constante.

Prenons pour H la classe unité H_0, on voit que

$$(2) \qquad \sum_{\mathfrak{p} \text{ dans } H_0} \frac{1}{(N\mathfrak{p})^s} = \frac{1}{h}\log\frac{1}{s-1} + f(s),$$

$f(s)$ est continue pour $s = 1$, si $L_k(1, \chi) \neq 0$ pour χ non principal; sans cela $f(s)$ tend vers $-\infty$ quand s tend vers 1.

Soit K un sur-corps galoisien de k de degré relatif n; on déduit aisément de (1), quand on l'applique à $\zeta_k(s)$, que

$$(3) \qquad \sum \frac{1}{(N\mathfrak{p}_1)^{-s}} = \frac{1}{n}\log\frac{1}{s-1} + g(s),$$

la somme étant étendue aux idéaux de k qui se décomposent dans K en un produit d'idéaux premiers tous différents de degré relatif 1; $g(s)$ étant continue pour $s = 1$.

Définition. — *Le groupe d'idéaux formé des classes suivant le rayon* (mod $\tilde{\mathfrak{f}}$) *contenant des normes d'idéaux de* K *est dit le groupe d'idéaux* (mod $\tilde{\mathfrak{f}}$) *attaché à* K.

Comme tous les $\mathfrak{p}_1$ sont des normes de K, si l'on prend pour H_0 ce groupe d'idéaux, la comparaison de (2) et de (3) montre que :

6° *L'indice du groupe d'idéaux* (mod $\mathfrak{f}$) *attaché à* K *est au plus égal au degré relatif de* K. *Si ces deux degrés sont égaux,* $L_k(1, \chi) \neq 0$ *pour un caractère* χ *non principal.*

Ce fait est fondamental dans la théorie du corps de classes.

Signalons que les fonctions ici étudiées ont été généralisées dans deux directions (Artin [2] ou Hasse [4, p. 146 et suiv.] : *voir* Chap. IV, § 5, et Hecke [3] et [4]).

XI. — Les analogies fonctionnelles et les nombres $\mathfrak{p}$-adiques.

Il y a entre la théorie des corps algébriques et celle des fonctions algébriques de profondes analogies (Hilbert [4; Pr. XII]) qui n'ont pas encore été complètement élucidées.

Considérons une surface de Riemann algébrique R de degré n; les fonctions algébriques définies sur cette surface forment (au sens du paragraphe 2), un corps.

Cette surface a m points à l'infini. Appelons « entiers » les fonctions n'ayant de pôles qu'en un de ces m points. On peut alors définir des idéaux, des idéaux premiers, etc. comme au paragraphe 6 et leur théorie est parallèle à celle des idéaux de la théorie des corps algébriques (Dedekind et Weber, [1]). Un idéal est formé de toutes les fonctions s'annulant en s points non à l'infini; si $s = 1$, l'idéal est premier : la notion d'idéal remplace ainsi celle de point, et permet de démontrer d'une manière complète et précise bien des théorèmes (comme le théorème de Riemann-Roch, par exemple).

Considérons une autre surface de Riemann $\overline{\mathrm{R}}$ telle que toute fonction de R soit uniforme sur $\overline{\mathrm{R}}$; elle définit un sur-corps de fonctions; et les points de ramificatiou correspondent aux idéaux de ramification.

Dans une autre direction se révèlent aussi des analogies formelles : on sait qu'on peut développer une fonction quelconque (en un point non-singulier de R et de la fonction) en série suivant les puissances de $x - x_0$. Soit de même un idéal premier $\mathfrak{p}$ d'un corps k; soit π un nombre de k divisible par $\mathfrak{p}$ et non par $\mathfrak{p}^2$; α un nombre quelconque de k que nous supposerons d'abord entier; on démontre sans peine qu'on peut trouver une série formelle

$$\alpha_0 + \alpha_1 \pi + \ldots + \alpha_p \pi^p + \ldots \tag{1}$$

telle que, pour tout p, on ait

$$\alpha \equiv \alpha_0 + \alpha_1 \pi + \ldots + \alpha_p \pi^p \pmod{\mathfrak{p}^{p+1}}. \tag{2}$$

Ce développement, qui exprime en quelque sorte la classe de congruence de α suivant toutes les puissances de $\mathfrak{p}$ ne doit pas être pris comme une véritable somme : c'est un simple symbole.

Une série quelconque de forme (1) ne correspond pas toujours à

un nombre α ayant pour tout p la propriété (2). Nous appelons une telle série un nombre $\mathfrak{p}$-adique.

Nous considérons aussi comme un nombre $\mathfrak{p}$-adique les développements de forme

$$\alpha_{-n}\pi^{-n} + \alpha_{-n+1}\pi^{-n+1} + \ldots.$$

Les nombres de forme (1) seront dits *entiers*. Deux nombres

$$\sum_{-n}^{\infty} \alpha_p \pi^p \quad \text{et} \quad \sum_{-n}^{+\infty} \beta_p \pi^p$$

sont dits *congrus* (mod $\mathfrak{p}^{i+1}$) si l'on a

$$\sum_{p=-n}^{p=i} \alpha_p \pi^{i+p} \equiv \sum_{p=-n}^{p=i} \beta_p \pi^{i+p} \qquad (\text{mod}\, \mathfrak{p}^{n+i+1}),$$

ils seront dits *égaux* s'ils sont congrus (mod $\mathfrak{p}^{j+1}$) quel que soit j.

Nous appliquerons à ces séries les règles ordinaires de calcul des séries convergentes. Les nombres $\mathfrak{p}$-adiques forment alors un corps au sens du paragraphe 2.

La théorie des corps et des entiers $\mathfrak{p}$-adiques peut alors se développer d'une manière semblable à la théorie ordinaire des corps algébriques (Hensel [1; 2; 3; 4; 5; 6]).

Des travaux de Öre [1] résulte que la méthode du développement de Puiseux au voisinage d'un point de ramification peut se transposer à ce cas.

Pour un autre point de vue dans la théorie des nombres $\mathfrak{p}$-adiques (qui consiste à regarder les éléments du corps algébrique comme les points d'un espace où la distance de α et β est w^a, si $(\alpha - \beta) = \mathfrak{p}^a \mathfrak{q}$ [$\mathfrak{q}$ entier pour $\mathfrak{p}$, $0 < w < 1$ et les nombres $\mathfrak{p}$-adiques comme les points-limites de ces points], consulter Hasse [24] et Chevalley [4].

CHAPITRE II.

LE CORPS DE CLASSES.

Le principal problème de la théorie des corps est le suivant : *soient k un corps, K un sur-corps; comment se décomposent les idéaux premiers de k dans* K ?

Ce problème n'a été traité que dans le cas où K est abélien par rapport à k [c'est-à-dire (Chap. 1, § 3_2) est galoisien et a un groupe de Galois abélien]; c'est la *théorie du corps de classes;* et tous les cas particuliers, qui avaient été étudiés avant l'édification de cette théorie et dont nous allons indiquer succintement les principaux, concernaient des corps relativement abéliens.

I. — Le corps circulaire des racines $m^{\text{ièmes}}$ de l'unité.

C'est le corps $k(\zeta)$, k étant le corps des rationnels, ζ une racine $m^{\text{ième}}$ primitive de l'unité. *Voir* Hilbert [1, 4e partie].

1. Ce corps est galoisien par rapport à k et a un groupe isomorphe au groupe multiplicatif des classes de congruence $(\bmod m)$, formées de nombres premiers à m; une substitution σ du groupe de Galois transforme ζ en ζ^a [a est une racine primitive $(\bmod m)$].

2. Le discriminant du corps ne contient que des nombres premiers figurant dans m $\Big[$pour le voir, le plus simple est de calculer le discriminant de l'équation $f(x) = x^m - 1 = 0$, qui est un multiple du discriminant du corps; c'est

$$\prod_{(a)} f'(\zeta^a) = \pm m^m\Big].$$

Les facteurs premiers de m sont donc les seuls qui se ramifient (d'après Chap. I, § 9).

3. Cherchons comment se décompose un nombre premier p premier à m.

Supposons que $\sigma = \left[\frac{K}{(p)}\right]$ transforme ζ en ζ^s; alors (Chap. 1, § 10) $\sigma\zeta = \zeta^s \equiv \zeta^p (\bmod p)$; donc $\zeta^{a-p} \equiv 1 (\bmod p)$; $1 - \zeta^{a-p}$ est donc divisible par p; or la norme absolue divise $\prod_{u \neq 0} (1 - \zeta^u) = m$ comme le montre un calcul facile, sauf si $a \equiv p (\bmod m)$. Donc :

La substitution $\left[\frac{K}{(p)}\right]$ *transforme* ζ *en* ζ^p; *tous les* p *pour*

lesquels $\left[\frac{k}{(p)}\right]$ *est le même sont donc congrus entre eux* $(\bmod m)$ *et réciproquement.*

On déduit de là le groupe de décomposition de p et sa décomposition (Chap. I, § $9_{2\alpha}$); en particulier :

Pour que p se décompose en un produit d'idéaux différents du premier degré, il faut et il suffit que $p \equiv 1 \pmod m$.

Des faits exactement semblables se produisent quand on adjoint ζ à un corps quelconque ne le contenant déjà pas (Hasse [2, p. 39], Artin [4], ou Chevalley [4]).

II. — Corps quadratiques.

Pour ce paragraphe, *voir* Hilbert [1, 3e partie].

k étant le corps des rationnels, m un entier qui n'est pas divisible par un carré, appelons K le corps $k(\sqrt{m})$.

1. Ce corps est galoisien de degré relatif 2 par rapport à k; soient 1 et σ les éléments du groupe de Galois, $\sigma\sqrt{m} = -\sqrt{m}$.

2. Un calcul simple montre qu'une base des entiers (Chap. I, § 4_2) est formée par 1 et ω, $\omega = \sqrt{m}$, si $m \not\equiv 1 \pmod 4$, et $\omega = \frac{1+\sqrt{m}}{2}$ si $m \equiv 1 \pmod 4$.

3. On déduit le discriminant par la formule (Chap. I, § 8_{2c}), dans le premier cas il vaut $4m$; dans le second cas, m.

Les seuls nombres premiers ramifiés sont donc ceux qui divisent m, et éventuellement 2.

4. Soit p un nombre premier différent de ceux-là; si $\left(\frac{K}{p}\right) = \sigma$, on a $\sigma\sqrt{m} = -\sqrt{m} \equiv \sqrt{m}^p \pmod p$; donc $m^{\frac{p-1}{2}} \equiv -1 \pmod p$; au contraire, on voit de même que si $\left(\frac{K}{p}\right) = 1$, on aura $m^{\frac{p-1}{2}} \not\equiv +1 \pmod p$.

Ceci nous incite à introduire le symbole quadratique de Gauss $\left(\frac{m}{p}\right)$;

il vaut $+1$ si m est congru à un carré $(\bmod p)$; -1 dans le cas contraire [c'est un caractère du groupe multiplicatif des classes de congruence $(\bmod p)$]. On sait que (et nous allons le redémontrer bientôt dans un cas plus général) $\left(\frac{m}{p}\right)=+1$ ou -1 selon que $m^{\frac{p-1}{2}}\equiv+1$ ou -1 $(\bmod p)$. Donc (en tenant compte du Chapitre I, § 9_{2d}) :

p se décompose en un produit de deux idéaux premiers du premier degré si $\left(\frac{m}{p}\right)=+1$; il est premier dans K *si* $\left(\frac{m}{p}\right)=-1$.

5. Mais, on peut transformer cette condition, grâce à la loi de réciprocité quadratique. On peut, comme l'on sait définir $\left(\frac{m}{n}\right)$ pour n non premier, en convenant que $\left(\frac{m}{a}\right)\left(\frac{m}{b}\right)=\left(\frac{m}{ab}\right)$, on peut même supposer n négatif en convenant que $\left(\frac{m}{-n}\right)=\left(\frac{m}{n}\right)$; on sait que

$$(1)\qquad \left(\frac{a}{b}\right)\left(\frac{b}{a}\right)=(-1)^{\frac{a-1}{2}\frac{b-1}{2}+\frac{\operatorname{sgn}a-1}{2}\frac{\operatorname{sgn}b-1}{2}}$$

(a et b étant deux entiers impairs différents de ± 1; $\operatorname{sgn}a=+1$ si $a>0$, $\operatorname{sgn}a=-1$ si $a<0$)

$$(2)\qquad \left(\frac{-1}{a}\right)=(-1)^{\frac{a-1}{2}},$$

$$(3)\qquad \left(\frac{2}{a}\right)=(-1)^{\frac{a^2-1}{8}}$$

Supposons pour simplifier p impair et $m\equiv 1 \pmod 4$; alors, d'après (1),

$$\left(\frac{m}{p}\right)\left(\frac{p}{m}\right)=1.$$

On voit donc *dans ce cas pour que p se décompose en un produit de deux idéaux premiers du premier degré, il faut et il suffit que* $\left(\frac{p}{m}\right)=1$. *Si un p possède cette propriété, il en est de même de ceux qui lui sont congrus* $(\bmod m)$.

Dans tous les cas, on constaterait un fait semblable : seulement au lieu du module m, il faudrait prendre le module $4m$.

Ici encore, ce sont des conditions de congruence qui déterminent la décomposition.

6. Hilbert a donné un énoncé remarquable, fondant en une seule

les lois de réciprocité (1), (2) et (3), par l'introduction du *symbole de reste normique* [1] $\left(\frac{n, m}{w}\right)$, w étant un nombre premier; ce symbole vaut $+1$, si n est congru à la norme d'un nombre du corps $k(\sqrt{m})$ $(\bmod w^i)$, quel que soit i, et vaut -1 dans le cas contraire. Ce symbole a les propriétés suivantes :

$$(4)\qquad \left\{\begin{array}{l} \left(\frac{n, m}{w}\right)\left(\frac{m, n}{w}\right) = 1, \\ \left(\frac{nn', m}{w}\right) = \left(\frac{n, m}{w}\right)\left(\frac{n', m}{w}\right), \\ \left(\frac{n, mm'}{w}\right) = \left(\frac{n, m}{w}\right)\left(\frac{n, m'}{w}\right), \\ \left(\frac{-m, m}{w}\right) = 1, \qquad \left(\frac{n, w}{w}\right) = \left(\frac{n}{w}\right), \end{array}\right.$$

$\left(\frac{n, m}{w}\right) = 1$ si n et m sont premiers à w, et w impair.

On peut de plus calculer directement la valeur de ce symbole pour $w = 2$; les règles précédentes permettent alors de le calculer dons tous les cas.

$\tilde{\mathfrak{p}}_\infty$ étant l'idéal infini de k, on pose de même $\left(\frac{n, m}{\tilde{\mathfrak{p}}_\infty}\right) = 1$ sauf si m et n sont négatifs, auquel cas on convient que ce symbole vaut -1; on voit sans peine que ce dernier cas est le seul où n n'est pas congru $(\bmod \tilde{\mathfrak{p}}_\infty)$ à une norme [c'est-à-dire (Chap. I, § 7_3) de même signe qu'elle].

On voit que, n et m étant fixes, $\left(\frac{n, m}{p}\right)$ n'est égal à -1 que pour un nombre fini de nombres premiers p; et l'on a d'après (1), (2) et (3), par un calcul simple,

$$(5)\qquad \prod_{(p)}\left(\frac{n, m}{p}\right) = +1,$$

p parcourant tous les nombres premiers, et $\tilde{\mathfrak{p}}_\infty$.

Réciproquement on peut tirer de là (1), (2) et (3), en prenant pour n et m des valeurs convenables; (5) sera considéré comme la loi générale de réciprocité.

---

[1] Indiquons dès maintenant que l'on dit couramment qu'un nombre est « reste normique », « reste de $l^{\text{ième}}$ puissance », au lieu de dire qu'il est congru à une norme, ou à une $l^{\text{ième}}$ puissance.

Nous sommes parti dans ce qui précède de la loi de réciprocité supposée connue. Mais, réciproquement, si l'on peut démontrer directement (5), on retournera à ces lois : ce sera le chemin qu'il nous faudra suivre dans les cas les plus généraux.

On voit bien par ces résultats le lien entre les lois de décomposition et les lois de réciprocité.

III. — Corps kummériens.

Dans le cas particulier de m premier, *voir* Hilbert [1, 5e partie], Hecke [1, p. 148]; cas général dans Hasse [4, p. 41], Chevalley [4].

Soit k un corps contenant une racine $m^{\text{ième}}$ primitive de l'unité; α un nombre de k qui n'est pas une $m^{\text{ième}}$ puissance; K le corps $k(\sqrt[m]{\alpha})$. Ce corps est galoisien par rapport à k, de groupe relatif cyclique; une substitution de groupe change $\sqrt{\alpha}$ en $\zeta^a\sqrt{\alpha}$; appelons σ subtitution qui change $\sqrt{\alpha}$ en $\zeta\sqrt{\alpha}$ (1*).

On démontre que tout corps relativement cyclique de degré m par rapport à un tel corps k est de cette forme.

Si m est premier, tout corps relativement galoisien de degré m est relativement cyclique; ces corps avaient été étudiés pour la première fois par Kummer, dans le cas particulier où k est le corps étudié au paragraphe 1 des racines $m^{\text{ièmes}}$ de l'unité; d'où le nom de *corps kummériens*.

On prouve sans peine que le discriminant relatif n'est divisible que par des idéaux premiers divisant m ou α. Pour les autres, nous allons généraliser les considérations de la quatrième partie du paragraphe précédent.

Soit $\mathfrak{p}$ un tel idéal premier; soit $\left(\frac{\alpha}{\mathfrak{p}}\right) = \sigma^a$; on a

$$\sigma^a \sqrt[m]{\alpha} \equiv (\sqrt[m]{\alpha})^{N\mathfrak{p}} \pmod{\mathfrak{p}},$$

$N\mathfrak{p}$ étant la norme absolue de $\mathfrak{p}$. Donc

$$\zeta^a \equiv \alpha^{\frac{N\mathfrak{p}-1}{m}} \pmod{\mathfrak{p}}. \tag{1}$$

(1*) Herbrand suppose ici que α n'est pas de la forme β^d, d divisant m; ce qui résulte de l'hypothèse déjà faite si m est premier.

Nous poserons par convention

$$\left(\frac{\alpha}{\mathfrak{p}}\right) = \zeta^a = \frac{\sigma^a \sqrt[m]{\alpha}}{\sqrt[m]{\alpha}}.$$

Remarquons que les $\zeta^i (i = 0, 1, \ldots, m-1)$ fournissent un sous-groupe du groupe multiplicatif des classes de congruences (mod $\mathfrak{p}$) qui est d'ordre $N\mathfrak{p} - 1$ (Chap. I, § 7_2); ce sous-groupe est d'ordre m, car $1 - \zeta^i \not\equiv 0 \pmod{\mathfrak{p}}$, puisque $1 - \zeta^i$ divise m d'après le paragraphe 1; donc $N\mathfrak{p} - 1$ est divisible par m. On peut dès lors démontrer que :

Pour que α soit reste de $m^{\text{ième}}$ puissance (mod $\mathfrak{p}$) (*voir* la note p. 30), *il faut et il suffit que* $\left(\frac{\alpha}{\mathfrak{p}}\right) = 1$.

En effet, le groupe multiplicatif des classes de congruence (mod $\mathfrak{p}$) est cyclique (Chap. I, § 7_2); soit ρ un élément qui l'engendre; pour que $\alpha \equiv \rho^{mx} \pmod{\mathfrak{p}}$, il faut et il suffit évidemment que $\alpha^{\frac{N\mathfrak{p}-1}{m}} \equiv 1 \pmod{\mathfrak{p}}$; d'où le résultat.

$\left(\frac{\alpha}{\mathfrak{p}}\right)$ est dit, à cause de cette propriété, *symbole de $m^{\text{ième}}$ puissance*, Quand $m = 2$ et que k est le corps des rationnels, on retrouve le symbole habituel de reste quadratique.

De (1) résulte en outre :

1° $$\left(\frac{\alpha}{\mathfrak{p}}\right) = \left(\frac{\alpha'}{\mathfrak{p}}\right) \quad \text{si} \quad \alpha \equiv \alpha' \quad (\text{mod } \mathfrak{p}).$$

2° $$\left(\frac{\alpha}{\mathfrak{p}}\right)\left(\frac{\beta}{\mathfrak{p}}\right) = \left(\frac{\alpha\beta}{\mathfrak{p}}\right)$$

donc $\left(\frac{K}{\mathfrak{p}}\right)$ *est un caractère du groupe multiplicatif des classes de congruence* (mod $\mathfrak{p}$).

De la manière dont on a introduit le symbole résulte que $\left(\frac{\alpha}{\mathfrak{p}}\right) = \zeta^a$, si $\left(\frac{K}{\mathfrak{p}}\right)$ transforme $\sqrt[m]{\alpha}$ en $\zeta^a \sqrt[m]{\alpha}$. En particulier (Chap. I, § 9_{2d}) :

Pour que $\mathfrak{p}$ se décompose en idéaux différents du premier degré, il faut et il suffit que $\left(\frac{\alpha}{\mathfrak{p}}\right) = 1$.

Mais ici nous n'avons plus à l'avance de loi de réciprocité comme dans le cas précédent.

Hilbert a pourtant réussi dans certains cas particuliers ($m = 2$ [2, 3], ou bien m premier, k corps des racines $m^{\text{ième}}$ de l'unité, sous la condition que son nombre de classes soit premier à m [1, 5e partie]) et Furtwängler [4, 6] dans le cas général de m premier, à introduire un symbole normique $\left(\frac{\alpha, \beta}{\mathfrak{p}}\right)$ qui est une racine $m^{\text{ième}}$ de l'unité, qui ne vaut 1 que si β est congru à la norme d'un nombre de $k(\sqrt[m]{\alpha})$ (mod $\mathfrak{p}^i$), pour tout i, et qui satisfait aux formules (4) du paragraphe 2.

De plus la formule de réciprocité (5) se généralise aussi.

La démonstration de ces faits est longue et délicate; Hensel [7], Hasse [5, 6, 7, 8] ont défini et étudié directement ce symbole; mais les connaissances actuelles permettent d'éviter la théorie délicate de ce symbole comme nous le verrons au chapitre suivant.

On peut alors généraliser les lois de réciprocité (1), (2) et (3) du paragraphe 2. Nous reviendrons plus loin sur tout cela.

IV. — Le corps de classes.

Pour toute la fin de ce chapitre, nous renvoyons une fois pour toutes à Hasse [2, 3], qui contient un exposé complet (ou Takagi [1], ou Chevalley [4]).

Dans tous les cas particuliers précédents, s'est révélé le fait que : *la décomposition des idéaux premiers dépend de leurs propriétés de congruence suivant un certain module.* Plus exactement, $\left(\frac{K}{\mathfrak{p}}\right)$ était le même pour tous les idéaux premiers $\mathfrak{p}$ du corps de base congrus entre eux suivant un certain module.

Un fait semblable s'était produit dans l'étude entreprise par Hilbert [3] et terminée par Furtwängler [1, 2, 3] des corps abéliens par rapport à un corps k, et non ramifiés par rapport à k. Takagi, réunissant tout ce que l'on savait jusque-là, par une modification du principe des méthodes de démonstration, et une utilisation judicieuse des notions jusque-là connues, a démontré les théorèmes suivants qui généralisent et précisent ces faits :

Définition. — *Un corps* K *relativement galoisien par rapport*

à k est dit corps de classes de k pour le groupe d'idéaux H *de conducteur* $\tilde{\mathfrak{f}}$, *si :*

a. Toutes les normes par rapport à k d'idéaux de K *premiers à* $\mathfrak{f}$ *sont dans* H;

b. L'ordre h de $A_{\tilde{\mathfrak{f}}}$: H($A_{\tilde{\mathfrak{f}}}$ *étant le groupe des idéaux de k premiers à* $\tilde{\mathfrak{f}}$), *donc l'indice de* H *est égal au degré relatif de* K *par rapport à k.*

D'après le Chapitre I, paragraphe 10_6, cet indice ne peut être supérieur à n.

1. *A tout groupe d'idéaux* H *correspond un corps* K *et un seul qui est corps de classes pour k.*

2. *Le groupe de Galois de* K *par rapport à k est isomorphe au groupe* $A_{\tilde{\mathfrak{f}}}$: H.

3. *Le conducteur* $\tilde{\mathfrak{f}}$ *et le discriminant relatif généralisé* $\tilde{\delta}$ *de* K *par rapport à k, sont divisibles par les mêmes idéaux premiers (généralisés).*

Il est indiqué pour la suite de diviser cet énoncé en deux :

a. Tout idéal premier divisant $\tilde{\mathfrak{f}}$ *divise* $\tilde{\delta}$.

b. Tout idéal premier divisant $\tilde{\delta}$ *divise* $\tilde{\mathfrak{f}}$.

$\tilde{\mathfrak{f}}$ est dit le conducteur de K par rapport à k (ou le conducteur, simplement, quand aucune confusion n'est possible).

4. (Umkehrsatz de Takagi). *Tout sur-corps abélien de k est corps de classes de k pour un certain groupe d'idéaux* H.

Ce sont là les théorèmes fondamentaux qui donnent comme on le voit une vue complète sur tous les sur-corps abéliens de k.

Nous résumerons plus loin leur démonstration. En voici une conséquence qui les précise. (On la démontre par un artifice simple.)

5. *Conservant les mêmes notations,* $\mathfrak{p}$ *étant un idéal premier de k premier à* $\tilde{\mathfrak{f}}$, $\mathfrak{p}^f$ *la plus petite puissance de* $\mathfrak{p}$ *qui est dans* H,

alors $\mathfrak{p}$ *se décompose dans* K *en un produit d'idéaux premiers différents de degré* f *par rapport à* k.

Pour la décomposition des idéaux premiers divisant $\tilde{\mathfrak{f}}$, *voir* Hasse [**2**, p. 30]. D'après le Chapitre I (§ $10_{5,6}$), de **1** résulte le théorème généralisé de la progression arithmétique. Une autre méthode pour le démontrer est la suivante : considérons les différents caractères non principaux χ du groupe $A_{\tilde{\mathfrak{f}}} : H$; chacun a un conducteur $\tilde{\mathfrak{f}}_\chi$ considérons la série $L_k(s, \chi)$ définie $(\text{mod } \tilde{\mathfrak{f}}_\chi)$ [qui correspond donc à un caractère propre $(\text{mod } \tilde{\mathfrak{f}}_\chi)$, et ne diffère que par un nombre fini de facteurs de la série $L(s, \chi)$ définie $(\text{mod } \tilde{\mathfrak{f}})$]; à partir de **5** et de sa généralisation aux idéaux premiers de $\tilde{\mathfrak{f}}$, on déduit sans peine

$$\zeta_K(s) = \zeta_k(s) \Pi_\chi L(s, \chi),$$

$\zeta_k(s)$ et $\zeta_K(s)$ étant les fonctions ζ des corps k et K. Ces fonctions ayant un pôle simple en $s = 1$, on en déduit que $L_k(s, \chi) \neq 0$ pour $s = 1$; on a vu que de là aussi résulte le théorème généralisé de la progression arithmétique.

Une autre conséquence est la suivante :

6. *Si* K *et* K′ *sont les corps de classes de* k *correspondant aux groupes* H *et* H′, KK′ *correspond au groupe formé des éléments communs à* H *et* H′; *et le plus grand sous-corps de* K *et* K′ *correspond au plus petit groupe d'idéaux contenant* H *et* H′.

Ce théorème exprime en quelque sorte « l'isomorphie » entre corps et groupes.

L'originalité de Takagi dans cette théorie fut de mettre à la base la définition déjà indiquée du corps de classes et de démontrer d'abord les théorèmes I à IV; et ce n'est qu'ensuite, contrairement à ses devanciers, qu'il démontre **5**. Il démontre d'abord [avec les fonctions $\zeta(s)$] le lemme suivant, qui est un cas particulier de **6** :

6 *bis*. K et K′ *étant corps de classes correspondant aux groupes* H *et* H′, $H \subset H'$, $H = H'$, $H \supset H'$ *entraînent respectivement* $K \supset K'$, $K = K'$, $K \subset K'$, *et réciproquement*.

Ceci justifie notre définition de l'égalité de deux groupes. Puis il

démontre les théorèmes I à IV par récurrence sur le degré relatif (*voir* les paragraphes suivants), toute la difficulté se concentrant sur le cas d'un degré relatif premier.

Il est intéressant de considérer des cas particuliers des théorèmes fondamentaux. D'après 3, si $\tilde{\mathfrak{f}} = (1)$, $\tilde{\delta} = (1)$ et réciproquement. Donc pour un corps relativement abélien non ramifié, H est composé de classes au sens ordinaire; et la décomposition d'un idéal premier dépend de sa classe au sens ordinaire. Prenons en particulier pour H le groupe des idéaux principaux; K est le plus grand sur-corps abélien de k non ramifié. Si nous prenons pour H le groupe des idéaux (α) où α est totalement positif, K sera le plus grand sur-corps abélien de k, où seuls les idéaux infinis se ramifient. C'est le corps de classes « absolu » de k, déjà étudié par Hilbert.

Le mot de « corps de classes » provient de la théorie de la multiplication complexe des fonctions elliptiques, où l'on étudiait les sur-corps abéliens de corps quadratiques imaginaires, et où les faits fondamentaux avaient été reconnus pour la première fois.

V. — Cas du degré relatif l premier (1*).

1. On commence par établir dans ce cas les théorèmes IIIa et IV du paragraphe précédent.

La démonstration consiste en une généralisation de la théorie de Gauss des genres des formes quadratiques, traduite dans le langage de la théorie des idéaux.

On commence (grâce à la théorie des groupes d'inertie et de ramification) par montrer que le discriminant $\tilde{\delta}$ est de forme $\tilde{\mathfrak{f}}^{l-1}$ ($\tilde{\mathfrak{f}}$ sera justement le conducteur du groupe d'idéaux correspondant K; mais, pour le moment, il n'y a pas d'autre signification que celle résultant de cette définition).

Soient :

$A_{\tilde{\mathfrak{f}}}$ le groupe des idéaux de k premiers à $\tilde{\mathfrak{f}}$;
A le groupe des idéaux de K;
$\tilde{H}_0$ la classe principale de K (au sens ordinaire);

(1*) *Voir* l'Appendice à propos des paragraphes V et VI.

H_1 le groupe des rayons $(\text{mod } \tilde{\mathfrak{f}})$ contenant des normes d'éléments de $\overline{H}_0$;

$H_{\tilde{\mathfrak{f}}}$ le groupe des rayons $(\text{mod } \tilde{\mathfrak{f}})$ contenant des normes d'éléments de $\overline{A}$;

$\overline{H}_1$ le groupe des idéaux de K dont la norme est dans H_1 (on appelle $\overline{H}_1$ le *genre principal*);

$\overline{H}_1$ contient évidemment $\overline{H}_0$.

σ étant une substitution engendrant le groupe de Galois, soit $\overline{H}'_1$ le groupe des classes de K (au sens ordinaire), de forme $A(\sigma A)^{-1}$, A étant une classe quelconque. $\overline{H}'_1$ est évidemment dans H_1, la norme d'un idéal de forme $\mathfrak{a}(\sigma\mathfrak{a})^{-1}$ valant 1.

L'ordre a de $\overline{A} : \overline{H}'_1$ est, on le voit aisément, égal au nombre des classes ambiges de K, c'est-à-dire des classes A telles que $A = \sigma A$.

En prenant les normes des éléments de $\overline{A}$, on voit que $\overline{A} : \overline{H}_1$ est isomorphe à $H_{\tilde{\mathfrak{f}}} : H_1$; donc ces deux groupes ont même ordre. Soit h_1 l'ordre de $A : H_1$; $h_{\tilde{\mathfrak{f}}}$ celui de $A_{\tilde{\mathfrak{f}}} : H_{\tilde{\mathfrak{f}}}$; il nous suffit, pour démontrer les théorèmes III a et IV, de démontrer que $h_{\tilde{\mathfrak{f}}} = l$, car alors K sera corps de classes pour le groupe d'idéaux $H_{\tilde{\mathfrak{f}}}$ défini $(\text{mod } \tilde{\mathfrak{f}})$, et dont le conducteur exact divise $\tilde{\mathfrak{f}}$.

a. On peut calculer directement a et h_1; le calcul de a conduit à étudier certains groupes d'unités; celui de h_1 les restes normiques $(\text{mod } \tilde{\mathfrak{f}})$. Ces deux calculs sont délicats; ils montrent que

$$a \leqq \frac{h_1}{l};$$

b. D'après le Chapitre I (§ 10_6), on a

$$h_{\tilde{\mathfrak{f}}} \leqq l,$$

car $H_{\tilde{\mathfrak{f}}}$ est le groupe d'idéaux $(\text{mod } \tilde{\mathfrak{f}})$ attaché au corps K.

On déduit immédiatement de ces deux égalités que

$$h_{\tilde{\mathfrak{f}}} = l, \qquad a = \frac{h_1}{l}, \qquad H'_1 = H_1.$$

On a donc démontré ce qu'il fallait et l'on a de plus des résultats accessoires :

a. Le nombre des classes ambiges est la $l^{\text{ième}}$ partie du nombre des classes;

b. Toute classe du genre principal est de forme $A(\sigma A)^{-1}$.

Le calcul de a et h_1 montre que :

c. Toute unité reste normique $(\text{mod } \tilde{\mathfrak{f}})$ *est une norme.*

2. Il faut maintenant démontrer 1 et 3_b dans le cas du degré relatif l.

a. On commence par supposer que k contient les racines $l^{\text{èmes}}$ de l'unité. On cherche le nombre m_1 des sur-corps de degré relatif l et de discriminant $\tilde{\mathfrak{f}}^{l-1}$, et le nombre m_2 des groupes d'idéaux H définis $(\text{mod } \tilde{\mathfrak{f}})$ d'indice l.

Un sur-corps galoisien de degré relatif l est, dans le cas étudié, engendré par la racine $l^{\text{ième}}$ d'un élément de k (§ 3); le calcul du premier nombre exige l'étude approfondie de ces corps déjà esquissée au paragraphe 3.

Le calcul du deuxième nombre exige l'étude aisée des restes de $l^{\text{ième}}$ puissance $(\text{mod } \tilde{\mathfrak{f}})$.

La comparaison de ces deux nombres montre, grâce à un artifice (d'ailleurs évitable), que m_1 (le nombre des corps) est plus petit ou égal à m_2 (le nombre des groupes) : $m_1 \leqq m_2$.

Or, d'après le théorème IV démontré dans le cas du degré relatif l, à tout corps correspond un groupe : donc $m_2 \leqq m_1$.

Donc $m_1 = m_2$; il y a autant de corps de degré l de discriminant $\tilde{\mathfrak{f}}^{l-1}$ que de groupes d'indice l définis $(\text{mod } \tilde{\mathfrak{f}})$; d'où il suit qu'à tout groupe correspond un corps (c'est le théorème I), et que le discriminant ne contient que des facteurs premiers du conducteur (c'est le théorème III b).

b. Il est dès lors aisé de supprimer la restriction que k doit contenir les racines $l^{\text{ième}}$ de l'unité.

Les théorèmes I, II, III et IV sont donc démontrés dans le cas du degré premier.

VI. — Cas général.

a. On démontre bien aisément que le théorème I est vrai pour un groupe d'idéaux quelconque et que le corps de classes correspondant possède les propriétés exprimées par les théorèmes II et III *a*.

b. On voit sans peine (d'après le Chapitre I, § 1_4) qu'il suffit de démontrer les théorèmes III*b* et IV dans le cas d'un corps K, à groupe relatif cyclique de degré l^n pour passer de là au cas général (l premier).

On pourrait penser à généraliser à ce cas la méthode ayant réussi dans le cas du degré l. Il est probable que c'est dans cette direction que l'on trouvera la démonstration la plus simple.

Takagi a employé une autre méthode : considérons les groupes définis au début du paragraphe 5. Remplaçons dans leur définition $\tilde{\mathfrak{f}}$ par un idéal $\tilde{\mathfrak{m}}$ que nous laissons pour le moment indéterminé; remplaçons les mots « classe principale de K » par « rayon (mod $\tilde{\mathfrak{M}}$) », $\tilde{\mathfrak{M}}$ étant un idéal de K, pour le moment indéterminé, qui divise $\tilde{\mathfrak{m}}$.

On démontre alors par récurrence sur n, que l'on peut toujours choisir $\tilde{\mathfrak{m}}$ et $\tilde{\mathfrak{M}}$ de manière que toutes les propriétés énoncées au paragraphe 5_1 subsistent, et que $\tilde{\mathfrak{m}}$ ne soit divisible que par des idéaux premiers du discriminant; comme au paragraphe 5_1, on en déduit les théorèmes III *b* et IV.

Cette démonstration est assez délicate.

Maintenant les théorèmes I, II, III et IV sont démontrés dans le cas général. Nous allons montrer au chapitre suivant comment on peut les compléter par la théorie des lois de Réciprocité.

Remarques historiques. — Avant Takagi ces théorèmes n'avaient été établis que pour le corps de classes non ramifié et les divisions d'idéaux en classes de conducteur égal à (1), ou à un produit d'idéaux à l'infini (en langage actuel). Les principes furent posés par Hilbert [3], et Furtwängler [1, 2, 3] acheva les démonstrations. Pour la démonstration de III_a et IV dans le cas du degré relatif l, ils n'employaient pas la relation $h_{\mathfrak{f}} \leqq l$ mais ils commençaient par établir la loi générale de réciprocité, et déduisaient de là l'égalité $a = h_1 : l$. Cette méthode était délicate et compliquée. Une autre méthode à signaler est celle de Hecke [1; Chap. VIII] qui, dans le cas $l = 2$, par

l'étude des singularités de certaines séries Θ, démontre une loi généralisant les lois de réciprocité quadratique, et établit par là l'existence des sur-corps non ramifiés de degré 2, avec leurs propriétés caractéristiques. Un résultat accessoire intéressant de cette méthode est le suivant :

La différente d'un corps algébrique par rapport à un sous-corps est dans le carré d'une classe (au sens ordinaire).

CHAPITRE III.

LOIS DE RÉCIPROCITÉ.

I. — Loi de réciprocité de Artin.

Pour tout ce chapitre, consulter Hasse [4].

Soit K un sur-corps abélien de k, corps de classes pour le groupe d'idéaux H de K, de conducteur $\tilde{\mathfrak{f}}$; soit A le groupe des idéaux de k premiers à $\tilde{\mathfrak{f}}$. A:H est isomorphe au groupe de Galois; la question se pose de savoir si l'on peut réaliser d'une façon simple cette correspondance entre les éléments de ces deux groupes.

Dans le corps $K = k(\zeta)$ (k corps des rationnels, ζ racine $m^{\text{ième}}$ primitive de l'unité) la réponse est aisée : p étant un nombre premier ne divisant pas m, on a vu (Chap. II, § 9) en effet que la *substitution* $\sigma = \left(\frac{K \mid k}{(p)}\right)$ *transforme* ζ *en* ζ^p; f étant le degré d'un idéal premier de K divisant p par rapport à k, σ^f est (Chap. I, § 9_2) l'unité; donc $p^f \equiv 1 \pmod{m}$. Donc la norme de tout idéal premier ne divisant pas m (donc celle de tout idéal premier à m) est de la forme (a) avec $a > 0$, $a \equiv 1 \pmod{m}$; ces idéaux (a) forment un groupe d'idéaux H de k, d'indice m. D'après la définition du corps de classes, K est corps de classes de k correspondant à H. Pour tous les idéaux principaux d'une même classe, on a $p \equiv a \pmod{m}$, donc $\left(\frac{K \mid k}{(p)}\right)$ est le même; on fait correspondre cette substitution à la classe : on voit sans peine que cette correspondance réalise l'isomorphie du groupe des classes et du groupe de Galois.

Partant de ce cas particulier et des théorèmes de Takagi, Artin [4],

incité par l'étude de certaines séries de Dirichlet (*voir* Chap. IV, § 5_2), a démontré le théorème général suivant :

$\left(\frac{K \mid k}{\mathfrak{p}}\right)$ *est le même pour tous les idéaux premiers d'une même classe suivant* H; *et cette correspondance entre les groupes des classes suivant* H *et le groupe de Galois est une isomorphie.*

En particulier si $\frac{\mathfrak{p}_1\mathfrak{p}_2}{\mathfrak{p}_3}$ est dans H, on a

$$\left(\frac{K \mid k}{\mathfrak{p}_1}\right)\left(\frac{K \mid k}{\mathfrak{p}_2}\right) = \left(\frac{K \mid k}{\mathfrak{p}_3}\right).$$

C'est la loi de réciprocité de Artin, ainsi nommée car elle entraîne, comme nous allons voir, les lois ordinaires de réciprocité; elle peut être considérée comme le théorème fondamental de la théorie du corps de classes. Son lien avec les lois ordinaires de réciprocité est clairement montré par le fait suivant : supposons que k contienne les racines $m^{\text{ième}}$ de l'unité; $K = k(\sqrt[m]{\alpha})$ alors $\left(\frac{K \mid k}{\mathfrak{p}}\right)$, et par suite $\left(\frac{\alpha}{\mathfrak{p}}\right)$ (*voir* Chap. II, § 3), ne dépend que de la classe de $\mathfrak{p}$ dans la division des idéaux en classes correspondant au corps K. C'est là, en quelque sorte, une loi « implicite » de réciprocité que nous préciserons plus loin.

On peut rendre plus frappant l'énoncé de la loi de Artin, en définissant $\left(\frac{K \mid k}{\mathfrak{a}}\right)$ pour un idéal quelconque $\mathfrak{a}$, en convenant que

$$\left(\frac{K \mid k}{\mathfrak{a}}\right)\left(\frac{K \mid k}{\mathfrak{b}}\right) = \left(\frac{K \mid k}{\mathfrak{ab}}\right);$$

alors la loi de Artin est équivalente à l'affirmation que l'ensemble des $\mathfrak{a}$ pour lesquels $\left(\frac{K \mid k}{\mathfrak{a}}\right)$ est le même est identique à l'ensemble des $\mathfrak{a}$ appartenant à une classe suivant H.

II. — Loi de réciprocité de Hasse.

La Théorie des restes normiques est une conséquence simple de la loi de Artin. Le problème est le suivant : *Étant donné un corps k contenant les racines $m^{\text{ièmes}}$ de l'unité, définir un symbole de reste*

normique $\left(\frac{\beta, \alpha}{\tilde{\mathfrak{p}}}\right)$, *qui soit une racine* $m^{\text{ième}}$ *de l'unité, et possède toutes les propriétés énoncées au Chapitre* II, § 1_0.

Nous avons indiqué (Chap. II, § **3**) l'historique de la théorie de ce symbole avant Takagi; sur la base de la théorie de corps de classes, Takagi [**2**] réussit à simplifier beaucoup sa théorie dans le cas m premier; Hasse [**15**] l'étendit au cas m non premier; mais ensuite [**20**] il réussit à donner de toute la théorie un exposé très simple et très général, que nous allons résumer.

Soit d'une manière générale K un sur-corps abélien de k, de groupe de Galois G, de conducteur $\tilde{\mathfrak{f}}$; β étant un entier de k, $\tilde{\mathfrak{p}}$ un idéal premier, fini ou infini, on définit un symbole $\left(\frac{\beta, K \mid k}{\tilde{\mathfrak{p}}}\right)$ $\left[\text{ou, si l'on n'a pas à craindre d'ambiguité, } \left(\frac{\beta, K}{\tilde{\mathfrak{p}}}\right)\right]$ comme suit :

Soit $\tilde{\mathfrak{f}}_{\mathfrak{p}}$ *la plus haute puissance de* $\mathfrak{p}$ *contenue dans le conducteur. Déterminons* β_0 *par les conditions :*

$$\frac{\beta_0}{\beta} \equiv 1 \pmod{\tilde{\mathfrak{f}}_{\tilde{\mathfrak{p}}}}, \qquad \beta_0 \equiv 1 \pmod{\frac{\tilde{\mathfrak{f}}}{\tilde{\mathfrak{f}}_{\tilde{\mathfrak{p}}}}}.$$

(*Si* $\tilde{\mathfrak{p}}$ *ne divise pas* $\tilde{\mathfrak{f}}$, *la première congruence signifie par convention que* $\frac{\beta_0}{\beta}$ *est premier à* $\tilde{\mathfrak{p}}$.)

Soit $(\beta_0) = \mathfrak{p}^b \mathfrak{b}$ ($\mathfrak{b}$ *premier à* $\mathfrak{p}$). [*Si* $\tilde{\mathfrak{p}}$ *est infini*, $(\beta_0) = \mathfrak{b}$], on *pose*

$$\left(\frac{\beta, K \mid k}{\tilde{\mathfrak{p}}}\right) = \left(\frac{K \mid k}{\mathfrak{b}}\right).$$

(Ce dernier symbole a été défini pour $\mathfrak{b}$ non premier à la fin du paragraphe **1**.)

Notre nouveau symbole est donc un élément du groupe de Galois. On voit sans peine qu'il est indépendant du choix particulier de β_0.

Ce symbole n'est différent de l'élément unité que pour les idéaux $\tilde{\mathfrak{p}}$ divisant $\tilde{\mathfrak{f}}$ ou (α). On démontre aisément les propriétés suivantes :

$$\left(\frac{\beta_1 \beta_2, K}{\tilde{\mathfrak{p}}}\right) = \left(\frac{\beta_1, K}{\tilde{\mathfrak{p}}}\right)\left(\frac{\beta_2, K}{\tilde{\mathfrak{p}}}\right).$$

$$\left(\frac{\beta, K_1 K_2}{\tilde{\mathfrak{p}}}\right) = \left(\frac{\beta, K_1}{\tilde{\mathfrak{p}}}\right)\left(\frac{\beta, K_2}{\tilde{\mathfrak{p}}}\right).$$

3° $\left(\frac{\beta, K}{\tilde{\mathfrak{p}}}\right)$ ne dépend que de la classe de congruence $(\bmod \tilde{\mathfrak{f}})$ où se trouve β.

4° Si la plus haute puissance de $\mathfrak{p}$ divisant (β) est $\mathfrak{p}^b$ et si $\mathfrak{p}$ est premier à $\mathfrak{f}$, on a

$$\left(\frac{\beta, K}{\mathfrak{p}}\right) = \left(\frac{K}{\mathfrak{p}}\right)^{-b}.$$

5° Pour que $\left(\frac{\beta, K}{\tilde{\mathfrak{p}}}\right)$ soit l'élément unité, il faut et il suffit que β soit resté normique $(\bmod \tilde{\mathfrak{f}}_{\mathfrak{p}})$; il est alors reste normique suivant toute puissance de $\mathfrak{p}$.

On voit donc que l'on peut considérer ce symbole comme un *symbole de reste normique*.

6° β étant fixe, et $\tilde{\mathfrak{p}}$ variant, $\left(\frac{\beta, K}{\tilde{\mathfrak{p}}}\right)$ n'est différent de l'élément unité que pour un nombre fini d'idéaux $\tilde{\mathfrak{p}}$, et l'on a

$$\prod_{\mathfrak{p}} \left(\frac{\beta, K}{\tilde{\mathfrak{p}}}\right) = 1$$

si l'on désigne par 1 l'élément unité. C'est la *loi de réciprocité de Hasse*.

7° Quand β varie, $\left(\frac{\beta, K}{\mathfrak{p}}\right)$ parcourt le groupe de décomposition de $\mathfrak{p}$; si β parcourt seulement les nombres premiers à K, ce symbole parcourt le groupe d'inertie (si $\mathfrak{p}$ est un idéal infini [*voir* Hasse 4; p. 34]).

A partir de la théorie de ce symbole, Hasse développe la théorie « locale » du corps de classes (Hasse [21]; F. K. Schmidt [1]); c'est la théorie des extensions algébriques abéliennes des corps $\mathfrak{p}$-adiques. Tous les théorèmes de la théorie du corps de classes restent vrais dans ce cas; et l'on a d'ailleurs trouvé depuis des démonstrations directes (Chevalley [4]).

III. — Loi de réciprocité de Hilbert.

Supposons maintenant que k contienne les racines $m^{\text{ièmes}}$ de l'unité et que $K = k(\sqrt[m]{\alpha})$.

On pose

$$\left(\frac{\beta, \alpha}{\tilde{\mathfrak{p}}}\right) = \frac{\sigma(\sqrt[m]{\alpha})}{\sqrt[m]{\alpha}},$$

σ étant la substitution $\left(\frac{\beta, K \mid k}{\tilde{\mathfrak{p}}}\right)$. $\left(\frac{\beta, \alpha}{\tilde{\mathfrak{p}}}\right)$ est évidemment une racine de l'unité. C'est le *symbole de reste normique* (pour l'exposant m) (et il en résulte des propriétés que nous allons indiquer que, dans les cas particuliers étudiés au Chapitre II, l'ancien et le nouveau symbole normique coïncident).

Nous avons défini au Chapitre II (§ 3) le symbole de $m^{\text{ième}}$ puissance $\left(\frac{\alpha}{\mathfrak{p}}\right)$; nous étendrons la définition à des $\mathfrak{p}$ non premiers en convenant que

$$\left(\frac{\alpha}{\mathfrak{a}}\right)\left(\frac{\alpha}{\mathfrak{b}}\right)=\left(\frac{\alpha}{\mathfrak{ab}}\right).$$

On écrira $\left(\frac{\alpha}{\beta}\right)$ au lieu de $\left(\frac{\alpha}{(\beta)}\right)$; $\left(\frac{\alpha}{(1)}\right)$ $\left[\text{et donc } \left(\frac{\alpha}{\varepsilon}\right) \text{ pour toute unité } \varepsilon\right]$ sera donc considéré comme égal à 1.

1. Les propriétés 1, 2, 3, 4, 5, 6 du paragraphe précédent restent vraies en remplaçant partout dans les symboles K par α; $\left[\text{par exemple dans 4, au lieu de } \left(\frac{K}{\mathfrak{p}}\right), \text{ on aura le symbole de } m^{\text{ième}} \text{ puissance } \left(\frac{\alpha}{\mathfrak{p}}\right)\right]$.

En particulier,

$$\prod_{\tilde{\mathfrak{p}}}\left(\frac{\beta, \alpha}{\tilde{\mathfrak{p}}}\right)=1.$$

C'est la *loi de réciprocité de Hilbert :* on voit qu'elle est vraie dans les cas les plus généraux.

Pour interpréter les propriétés 3 et 4, on tiendra compte du fait que $\tilde{\mathfrak{f}}$ ne contient, d'après la théorie des corps kummériens, outre des idéaux infinis, que des facteurs premiers de α et de m.

2. On a

$$\left(\frac{\beta, \alpha}{\tilde{\mathfrak{p}}}\right)\left(\frac{\alpha, \beta}{\tilde{\mathfrak{p}}}\right)=1,$$

cela résulte de la formule évidente $\left(\frac{-\mu, +\mu}{\tilde{\mathfrak{p}}}\right)=1$.

3. On déduit de là que $\left(\frac{\beta, \alpha}{\tilde{\mathfrak{p}}}\right)$ ne dépend que de α et β $(\text{mod } \tilde{\mathfrak{p}})^a$,

a étant un nombre convenable dont on peut d'ailleurs préciser la valeur ($a = 1$, si $\tilde{\mathfrak{p}}$ est premier à m).

Nous avons donc toutes les propriétés exigées du symbole de reste normique.

IV. — Lois explicites de réciprocité.

En substituant à α et β des nombres convenables dans la loi de réciprocité de Hilbert et en tenant compte des propriétés de ce symbole, en particulier de la quatrième propriété du paragraphe 2, on trouvera les lois de réciprocité sous leur forme ordinaire. Nous considérons dans ce qui suit des symboles de $m^{\text{ième}}$ puissance, et des symboles de restes normiques pour l'exposant m.

Désignons par $\mathfrak{l}$ un facteur premier quelconque de m dans le corps étudié k. $\mathfrak{p}$ désignera désormais un idéal premier fini qui n'est pas un $\mathfrak{l}$. Prenons d'abord α et β premiers entre eux et à m. $\left(\frac{\beta, \alpha}{\mathfrak{p}}\right) = 1$, sauf quand $\mathfrak{p}$ divise α ou β, auquel cas la valeur de ce symbole est donnée (§ 2, 4°). Un calcul aisé donne

$$(1) \qquad \left(\frac{\alpha}{\beta}\right)\left(\frac{\beta}{\alpha}\right)^{-1} = \prod_{\mathfrak{l}} \left(\frac{\beta, \alpha}{\mathfrak{l}}\right) \prod_{\mathfrak{p}_\infty} \left(\frac{\beta, \alpha}{\tilde{\mathfrak{p}}_\infty}\right),$$

$\tilde{\mathfrak{p}}_\infty$ parcourant tous les idéaux à l'infini.

Prenons pour α un nombre premier à m, pour λ un nombre dont tous les facteurs idéaux premiers sont des $\mathfrak{l}$; on trouve de même

$$(2) \qquad \left(\frac{\lambda}{\alpha}\right)^{-1} = \prod_{\mathfrak{l}} \left(\frac{\lambda, \alpha}{\mathfrak{l}}\right) \prod_{\mathfrak{p}_\infty} \left(\frac{\lambda, \alpha}{\tilde{\mathfrak{p}}_\infty}\right).$$

Il est aisé de supprimer dans ces formules une partie des restrictions sur α et β.

Il faut calculer le deuxième membre de (1) et de (2).

a. $\left(\frac{\beta, \alpha}{\tilde{\mathfrak{p}}_\infty}\right)$ ne figure dans nos formules que si $m = 2$ (sans cela les racines $m^{\text{ièmes}}$ de l'unité sont par hypothèse dans le corps de base, qui est imaginaire avec tous ses conjugués). Il vaut donc $+1$ ou -1; il ne vaut -1 que si β n'est pas reste normique de $k(\sqrt{\alpha})$, $(\bmod \tilde{\mathfrak{p}}_\infty)$, ou si α n'est pas reste normique de $k(\sqrt{\beta})$ $(\bmod \tilde{\mathfrak{p}}_\infty)$ [c'est-à-dire

(Chap. I, § 7_3) qu'il n'y a pas de norme de même signe dans le corps réel conjugué correspondant à $\tilde{\mathfrak{p}}_\infty$]. On voit immédiatement que ce n'est possible que si les conjugués de α et β dans les corps (nous les désignerons par $\alpha^{(\tilde{\mathfrak{p}}_\infty)}$, $\beta^{(\tilde{\mathfrak{p}}_\infty)}$) sont négatifs. D'où

$$\left(\frac{\beta, \alpha}{\tilde{\mathfrak{p}}_\infty}\right) = (-1)^{\frac{\operatorname{sgn}\alpha^{(\tilde{\mathfrak{p}}_\infty)}-1}{2}\,\frac{\operatorname{sgn}\beta^{(\tilde{\mathfrak{p}}_\infty)}-1}{2}} \qquad \left(\text{où } \operatorname{sgn} x = \frac{x}{|x|}\right).$$

b. On sait que $\left(\frac{\beta, \alpha}{\mathfrak{l}}\right)$ ne dépend que de la classe de congruence de α et β modulo une certaine puissance de $\mathfrak{l}$ (§ 3_3).

On voit en définitive que les seconds membres de (1) et (2) ont une valeur qui est déterminée par la classe de congruence de α et β modulo un certain idéal $\mathfrak{a}$, et par les signes des conjugués réels de α et β.

Par exemple, si m est un nombre premier l, on démontre que, dans (1), $\mathfrak{a} = (l)$; et dans (2), $\mathfrak{a} = (l)(1-\zeta)$ (ζ racine $l^{\text{ième}}$ primitive de 1).

On a donc une parfaite généralisation des lois de réciprocité : 1° correspond à la loi générale de réciprocité; quand β est une unité, on a $\left(\frac{\alpha}{\beta}\right) = 1$ et on a la généralisation de la première loi complémentaire; enfin 2° généralise la deuxième loi complémentaire.

Il reste à obtenir la valeur explicite de $\left(\frac{\beta, \alpha}{\mathfrak{l}}\right)$ en fonction de β et α. Ce difficile problème a été abordé par Hasse [9, 10, 11, 12, 13, 14, 16, 17] dans une série de Mémoires, et n'est que partiellement résolu.

Pour un exposé systématique, consulter Hasse [4], les formules générales utilisent des notions empruntées à la théorie des corps $\mathfrak{p}$-adiques, qu'il serait trop long d'indiquer ici.

Signalons enfin que, par des méthodes transcendantes, on peut obtenir des cas particuliers de ces lois (Hecke [1, Chap. VIII]; Fueter [3]).

V. — Application au théorème de Fermat.

Beaucoup de critères pour l'impossibilité en entiers rationnels de l'équation

$$x^l + y^l = z^l \qquad (l \text{ premier}) \tag{1}$$

peuvent se déduire des lois explicites de réciprocité de la façon suivante : de (1), on déduit

$$\prod_{i=0}^{i=l-1} (x + \zeta^i y) = (-z)^l,$$

alors on voit que les $x + \zeta^i y$ sont des $l^{\text{èmes}}$ puissances d'idéaux, ainsi donc que

$$\alpha = \frac{x + \zeta y}{x + y} = 1 - \frac{y}{x + y}\lambda \qquad \{\alpha \equiv 1 [\operatorname{mod}(\lambda)]\},$$

où l'on a posé $\lambda = 1 - \zeta$. Donc $\left(\frac{\beta}{\alpha}\right) = 1$ pour tout $\beta \neq 0$ de k. En remplaçant β par des nombres particuliers, on aura des conditions nécessaires pour la résolubilité de (1); en prenant pour β des nombres premiers, on trouve comme conditions :

1° $\frac{p^{l-1} - 1}{l} \equiv 0 \pmod{l}$ pour tout diviseur premier p d'un des x, y, z premier à l; d'où :

2° $\frac{2^{l-1} - 1}{l} \equiv 0 \pmod{l}$ (critère de Wieferich);

3° On peut aussi démontrer $\frac{3^{l-1} - 1}{l} \equiv 0 \pmod{l}$ (critère de Mirimanoff); on a toute une série d'autres critères correspondants (*voir* Hasse [4; p. 113], Furtwängler [7]);

4° De 1° on déduit que $2l + 1$ n'est pas premier (critère de Legendre et Sophie Germain).

La théorie du corps de classes permet aussi de beaucoup simplifier la démonstration des lemmes nécessaires au deuxième critère de Kummer pour l'impossibilité de (1) quand z est divisible par l (Herbrand [2]).

CHAPITRE IV.

APPLICATIONS.

I. — Cas particuliers.

1. Prenons pour corps de base k_0 le corps des nombres rationnels. A tout sur-corps K correspond une division en classes définies $(\operatorname{mod} \mathfrak{f})$;

on peut toujours supposer que $\tilde{\mathfrak{f}}$ est le produit d'un idéal ordinaire (f) par l'idéal à l'infini (unique) de k (f étant un nombre entier positif). Soit $K_{\tilde{\mathfrak{f}}}$ le sur-corps abélien de k, qui est corps de classes pour le rayon $(\bmod \tilde{\mathfrak{f}})$. $K_{\tilde{\mathfrak{f}}} \supset K$, d'après le Chapitre II, § 4. Or, le rayon $(\bmod \tilde{\mathfrak{f}})$ est engendré par les idéaux (a), tels que $a > 0$ et $a \equiv 1 \pmod{f}$; d'après le Chapitre III, § 9, on voit que $K_{\tilde{\mathfrak{f}}}$ est le corps des racines $f^{\text{ièmes}}$ de l'unité. D'où un célèbre théorème de Kronecker :

Tout corps relativement abélien par rapport au corps des nombres rationnels est sous-corps d'un corps circulaire $k_0\left(e^{\frac{2\pi i}{f}}\right)$.

Bien des démonstrations compliquées avaient été précédemment données (par exemple Hilbert [1, Chap. XXIII], Weber [4], Speiser [2]).

2. Prenons pour corps de base k, un corps quadratique imaginaire $k_0(\sqrt{-m})$. Par une démonstration dont le noyau est identique à celui de la précédente, mais bien plus compliquée, on est parvenu (Weber [1], Fueter [2], Takagi [1], Hasse [23]), pour la première fois, grâce à la théorie du corps de classes, à démontrer complètement le :

Rêve de jeunesse de Kronecker. — *Tout corps relativement abélien par rapport à un corps quadratique imaginaire est sous-corps d'un corps obtenu en adjoignant à celui-là des racines de l'unité, et :*

a. Ou bien des valeurs « singulières » de la fonction modulaire $\mathfrak{p}(u)$ *et des racines carrées de nombres du domaine de rationalité ainsi déterminé;*

b. Ou bien encore, des valeurs « singulières » de la fonction $\tau(u)$ *définie par*

$$\tau(u) = \frac{g_2 g_3}{g_2^3 - 27 g_3^2}\,\mathfrak{p}(u),$$

sauf dans le cas $m = 1$, *où* $\tau(u) = \frac{\mathfrak{p}^2(u)}{g_2}$, *et le cas* $m = 3$, *où* $\tau(u) = -\frac{\mathfrak{p}^3(u)}{g_3}$.

Les valeurs « singulières » en question sont certaines valeurs particulières pour lesquelles u appartient à k.

Hilbert [4; Pr. 12] a posé le problème général suivant : *Est-il possible de trouver pour tout corps de base k des fonctions qui jouent le même rôle que les fonctions* $e^{2\pi i x}$, $j(x)$, $\tau(x)$, *dans les deux cas particuliers précédents.*

Le seul essai dans l'étude de ce problème a été fait par Hecke [2], dans le cas d'un corps de base quadratique réel.

3. Les corps non galoisiens de degré 3 par rapport au corps des rationnels ont été étudiés sommairement par les moyens de la théorie du corps de classes par Hasse [18].

II. — Différente et groupes de ramification.

1. La détermination de ces éléments a été faite par Hasse [22], [26]. Le résultat est le suivant :

Soient K *un sur-corps abélien de k,* H *le groupe d'idéaux correspondant de conducteur* $\mathfrak{f}$; *considérons tous les groupes d'idéaux plus grands que* H, *et* H *lui-même et tous leurs conducteurs; considérons les plus hautes puissances de* $\mathfrak{p}$ *par lesquelles ces conducteurs sont divisibles; soient* $\mathfrak{p}^{1+a_1}$, $\mathfrak{p}^{1+a_2}$, ... *celles de ces puissances qui sont différentes* $(0 \leqq a_1 < a_2 < \ldots)$; $H_{\nu+1}$ *le plus petit de ces groupes où cette puissance est* $\mathfrak{p}^{1+a_\nu}$; H_1 *le plus petit de ces groupes de conducteur premier à* $\mathfrak{p}$. *Soient* K_ν *le corps de classes correspondant à* H_ν, g_ν *le sous-groupe correspondant de Galois de* K *par rapport à k :*

a. g_1 *est le groupe d'inertie de* $\mathfrak{p}$; *soit* ep^{r_2} *son ordre* (*e premier à p*), *p étant le nombre premier contenu dans* $\mathfrak{p}$ (*d'après* Chap. I, § 9_{3a});

b. Les v_1 *premiers groupes de ramification coïncident avec* g_2; *les* v_2 *suivant avec* g_3, *etc. Si* p^{a_ν} *est l'ordre de* g_ν, *on a*

$$v_\nu = (a_\nu - a_{\nu-1})\, e p^{a_2 - a_\nu}$$

(*on convient que* $a_0 = 0$).

2. Une conséquence de ce théorème est la proposition suivante, qui fut d'abord démontrée par des méthodes transcendantes :

Considérons tous les systèmes différents de caractères du groupe des classes suivant H; *la différente est le produit de leurs conducteurs* (*il est presque évident d'ailleurs que le conducteur du corps est leur* P. P. C. M.).

3. Une autre conséquence est la suivante :

Soient $\overline{\mathrm{K}}$ *un corps intermédiaire*, $\tilde{\mathfrak{f}}$ *le conducteur de* K *par rapport à* k, $\widetilde{\mathfrak{M}}$ *celui de* K *par rapport à* $\overline{\mathrm{K}}$, $\widetilde{\mathfrak{m}}$ *celui de* K *par rapport à* k. *Soit* $\widetilde{\mathfrak{m}} = \tilde{\mathfrak{f}}\widetilde{\mathfrak{m}}_0$. *Alors* $\widetilde{\mathfrak{M}} = \mathfrak{F}\,\widetilde{\mathfrak{m}}_0$, *où* $\mathfrak{F}$ *est un idéal ordinaire* (*non généralisé*) *obtenu comme suit* (*voir* Chap. I, § 8_3) :

$\mathfrak{P}$ *étant un idéal premier de* $\overline{\mathrm{K}}$ *divisant l'idéal premier* $\mathfrak{p}$ *de* k, $\mathfrak{P}$ *ne divise* $\widetilde{\mathfrak{F}}$ *que si* $\mathfrak{p}$ *divise* $\tilde{\mathfrak{f}}$; *la plus haute puissance de* $\mathfrak{P}$ *qui divise* $\mathfrak{F}$ *est* $\mathfrak{P}^{1+\nu}$, ν *étant le nombre de groupes de ramification* (*d'ordre différent de* 1) *de* $\mathfrak{P}$ *par rapport à* k (Herbrand [3]).

III. — Passage à un sur-corps.

K, k et H conservant le même sens, soit Ω un sur-corps *quelconque* de K; il résulte de la théorie de Galois que $\mathrm{K}\Omega$ est abélien par rapport à Ω. On démontre que :

a. $\mathrm{K}\Omega$ *est un corps de classes sur* Ω *pour le groupe des idéaux de* Ω *dans les normes par rapport à* k *sont dans* H;

b. Donc le conducteur de $\mathrm{K}\Omega$ *par rapport à* Ω *divise celui de* K *par rapport à* k.

Ces théorèmes ont été d'abord démontrés par Hasse [19] ou [4, p. 145], en utilisant des théorèmes sur la « densité » de certains idéaux, puis directement par Herbrand [1] qui a précisé (f) dans certains cas.

c. Ils restent vrais si l'on considère des corps de nombres $\mathfrak{p}$-adiques, au lieu de corps de nombres ordinaires (Chevalley [1], [4]).

IV. — Applications diverses.

L'ensemble des théorèmes de Takagi, de la loi de réciprocité de Artin, et du théorème § 3_a de Hasse, forme un instrument extrêmement puissant pour étudier les questions les plus difficiles de la théorie des nombres. Les deux exemples suivants sont caractéristiques :

1. Les groupes des classes. — *Soient k un corps, K un sur-corps (quelconque), k' le plus grand sur-corps de k compris dans K, et qui soit abélien et non ramifié par rapport à k, n son degré relatif. Le groupe quotient du groupe des classes de k par un groupe d'ordre n est isomorphe à un sous-groupe du groupe des classes de* K (Herbrand [2], Chevalley [3]).

Si, en particulier, K est galoisien par rapport à k, on peut prendre pour k' le plus grand corps contenu dans tous les corps d'inertie. On déduit de là une généralisation d'un théorème de Kummer :

Le groupe des classes d'un sous-corps du corps des racines $l^{\text{ièmes}}$ de l'unité est un sous-groupe du groupe des classes de ce dernier (l premier) (déjà démontré d'une manière analogue par Furtwängler [5]).

2. Théorème des idéaux principaux. — Dans ce qui suit, le mot classe sera pris au sens ordinaire (mais on pourrait aussi le prendre au sens restreint).

Hilbert [3] avait prévu que :

THÉORÈME DES IDÉAUX PRINCIPAUX. — *Tout idéal de k est principal dans le corps de classes* K *correspondant à la classe principale de k.*

Ce théorème ne fut d'abord démontré que dans des cas particuliers (Furtwängler [8], Hasse [2, p. 45]). Ce ne fut que trente ans après que ce théorème fut ramené par Artin [6] à un théorème de théorie des groupes, qui fut démontré par Furtwängler [11].

Le raisonnement de Artin est le suivant : soit $\overline{K}$ le corps de classes de K correspondant à la classe principale de K. Cette classe étant

UNIVERSITÉ DE GRENOBLE I
LABORATOIRE
DE MATHÉMATIQUES PURES
INSTITUT FOURIER

invariante dans tout automorphisme de K par rapport à k, on en déduit sans peine que $\overline{K}$ est galoisien par rapport à k (Chap. II, § 4_{6bis}); soient G son groupe de Galois; g le groupe correspondant à K. Il suffit évidemment de démontrer que tout idéal premier $\mathfrak{p}$ de k devient principal dans K. Soient $\mathfrak{P}$ un des diviseurs premiers de k dans K, $\tilde{\mathfrak{P}}$ un des diviseurs premiers de $\mathfrak{P}$ dans $\overline{K}$. Soit $\left[\frac{\overline{K}\mid k}{\tilde{\mathfrak{P}}}\right] = \alpha$; soit $\mathfrak{p} = \mathfrak{P}_1\mathfrak{P}_2\ldots\mathfrak{P}_u$ la décomposition de $\mathfrak{p}$ en facteurs premiers de K ($\mathfrak{P}_1 = \mathfrak{P}$); et soit enfin $\alpha^f = \sigma$ la plus petite puissance de α qui soit dans g. D'après le Chapitre I, § 9_{3d}, on a $\left[\frac{\overline{K}\mid K}{\tilde{\mathfrak{P}}}\right] = \sigma = \left(\frac{\overline{K}\mid K}{\tilde{\mathfrak{P}}}\right)$. Dans le groupe quotient G : g, qui est abélien, le complexe de G suivant g qui contient α, engendre le groupe de décomposition de $\mathfrak{P}$ par rapport à k, que nous désignerons par (α). Décomposons G : g suivant ce groupe (Chap. I, § 1_2) :

$$G : g = (\alpha)\sigma_1 + (\alpha)\sigma_2 + \ldots + (\alpha)\sigma_u.$$

Nous pouvons considérer les σ_i comme des éléments de G, si nous convenons de représenter par la même lettre l'élément σ de G et le complexe élément de G : g qui contient σ. On peut alors supposer, comme l'on voit aisément, $\sigma_i\mathfrak{P} = \mathfrak{P}_i$, et, d'après le Chapitre I, § 9_{2e}, on a $\left(\frac{\overline{K}\mid K}{\sigma_i\mathfrak{P}}\right) = \sigma_i\alpha\sigma_i^{-1}$. Donc :

$$\left(\frac{\overline{K}\mid K}{\mathfrak{p}}\right) = \prod_{(i)} \sigma_i\alpha\sigma_i^{-1}.$$

Si l'on peut démontrer que cet élément est l'unité, nous aurons démontré le théorème en question, car d'après la loi de réciprocité de Artin, $\mathfrak{p}$ est alors dans le groupe d'idéaux de K correspondant à $\overline{K}$, c'est-à-dire dans la classe principale de K.

Or quelles sont les propriétés de G ? g est un sous-groupe invariant abélien; G : g est abélien; de plus, nous allons voir que g est le groupe des commutateurs (Chap. I, § 1_6) de G. Soit, en effet, g' un sous-groupe invariant de G, tel que G : g' soit abélien; il correspond (au sens du Chapitre I, § 3_3) à un sous-corps k' de K. D'après le Chapitre II, § 4_4, K est non ramifié par rapport à k, ainsi que $\overline{K}$ par rapport à K. On déduit sans peine du Chapitre I, § 8, qu'il en est de même de $\overline{K}$ par rapport à k, puis de k' par rapport à k. Donc,

d'après le Chapitre II, § 4_1, k' a par rapport à k le conducteur (1); il est donc corps de classes correspondant à un groupe d'idéaux formé de plusieurs classes (au sens restreint); d'après le Chapitre II, § 4_{6bis}, $k' \subset K$; donc (Chap. I, § 3_3) g est sous-groupe de g'. D'après le Chapitre I, § 1_6, g est donc bien le groupe des commutateurs.

On est donc ramené a démontrer le théorème suivant :

G *étant un groupe tel que son groupe des commutateurs* g *soit abélien*, α *étant un élément de* G, α^f *la plus petite puissance de* α *dans* g; *le groupe quotient* $G : g$ *se décomposant suivant le groupe cyclique* (α) *engendré par* α *de la manière suivante :*

$$G : g = (\alpha)\sigma_1 + (\alpha)\sigma_2 + \ldots + (\alpha)\sigma_u,$$

dans ces conditions, le produit $\prod_{(i)} \sigma_i \alpha \sigma_i^{-1}$ *est égal à l'unité.*

Ce théorème fut démontré par Furtwängler [11] d'une manière très compliquée et qu'il serait intéressant de simplifier (1).

Le paragraphe 2_3 permet aisément de généraliser (Herbrand [3]).

Soit K *le corps de classes correspondant au rayon* $(\text{mod}\, \tilde{\mathfrak{f}})$. *Tout idéal de* k *est principal dans* K, *et est dans le rayon* $(\text{mod}\, \mathfrak{F})$, $\mathfrak{F}$ *étant déduit de* $\tilde{\mathfrak{f}}$ *comme dans l'énoncé du paragraphe* 2_3 (*cf.* aussi Iyanaga [1]).

Le raisonnement de Artin indiqué ci-dessous est particulièrement remarquable, car il montre que sa loi de réciprocité permet de travailler avec des groupes non abéliens. On voit, de plus, sur cet exemple comment cette loi permet de ramener un problème sur les corps algébriques à un problème de théorie des groupes.

Un problème suscité par cette question est le suivant :

Problème des tours de corps de classes. — *Soit une suite de corps* $K_1, K_2, \ldots, K_i, \ldots$, *tels que* K_{i+1} *soit le corps de classes absolu de* K_i; *une telle suite s'arrête-t-elle toujours à un corps tel que* $K_i = K_{i+1}$ (*donc tel que tous ses idéaux soient principaux*), *ou y a-t-il de telles suites infinies?*

(1) Cette simplification vient d'être trouvée par M. Iyanaga.

Ce problème est irrésolu; on sait seulement qu'il y a de telles « tours » ayant autant d' « étages » que l'on veut (Scholz [2]).

Il ne faut pas croire que le corps de classes absolu soit le plus petit corps, où tous les idéaux du corps de base deviennent principaux; des exemples contraires ont été fournis par Furtwängler [8], Pollaczek [1], Scholz [2].

3. **Divers.** — Citons :

a. Une démonstration et une généralisation du Chapitre II, § 5_1, à partir des théorèmes fondamentaux de la théorie (Herbrand [3]);

b. Une démonstration et une précision du théorème terminant le Chapitre II, § 6, dans le cas des corps galoisiens à groupe métacyclique (Herbrand [4]);

c. Un travail de Tchebotareff [2] sur la structure du corps de classes absolu des corps galoisiens par rapport au corps des rationnels;

d. Une application particulièrement importante est le théorème suivant dû à Hasse (démontré dans [4, p. 38] pour le cas du degré relatif premier).

Quand un nombre est resté normique d'un sur-corps relativement cyclique K (mod $\mathfrak{a}$), *quel que soit l'idéal* $\mathfrak{a}$, *ce nombre est une norme d'un nombre de* K.

Ce théorème peut être faux pour un sur-corps abélien non cyclique;

e. On trouvera enfin dans Moriya [1] une série d'applications très simples à des théorèmes en partie déjà connus.

V. — Corps non abéliens.

Il est naturel d'essayer d'étendre cette théorie du corps de classes au cas de corps relativement galoisiens à groupe non abélien. Mais les essais dans cette direction n'ont pas conduit très loin, on n'a pu réussir qu'à étudier ce qui dépend des propriétés de corps intermédiaires à groupe abélien.

1. La théorie des restes normiques peut s'étendre (Chevalley [2]) grâce au paragraphe 3_c :

Soient K *un sur-corps galoisien de* k; $\mathfrak{P}$ *un idéal premier* (*fini*)

de K; K_z *le corps de décomposition correspondant* [*c'est-à-dire le corps qui, dans le groupe de Galois de* K, *correspond* (*au sens du Chap.* I, § 3_3) *au groupe de décomposition de* $\mathfrak{P}$]; $\overline{K}$ *le plus grand corps tel que* $K_z \subset \overline{K} \subset K$ *qui soit abélien par rapport à* K_z [*il correspond, dans le groupe de Galois de* K (*d'après le Chap.* I, § 1_6), *au groupe des commutateurs du groupe de décomposition*]; $\mathfrak{p}_z$ *l'idéal premier de* K_z *divisible par* $\mathfrak{P}$.

α *étant un nombre de* k *pour que, pour tout* x, *il y ait un* A *de* K *tel que* $\alpha \equiv N_{Kk}(A) \pmod{\mathfrak{P}^x}$ (*il suffit pour cela qu'il en soit ainsi pour une seule valeur de* x, *si elle est assez grande*), *il faut et il suffit que, pour tout* x, *il y ait un* $\overline{A}$ *de* $\overline{K}$ *tel que*

$$\alpha \equiv N_{\overline{K}K_z}(\overline{A}) \qquad (\mathrm{mod}\, \mathfrak{p}^x),$$

$\overline{K}$ étant un sur-corps abélien de K_z, on est ramené au cas abélien; on peut définir un symbole de restes normiques et les propriétés 1, 2, 3, 4, 5, 7 du Chapitre III, § 2. s'étendent (4 et 7 convenablement modifiés).

2. Une direction intéressante, quoiqu'elle n'ait encore fourni aucun résultat dans le présent problème, a été indiquée par Artin [2] par l'étude de ses séries L introduites à propos d'un problème sur les fonctions $\zeta(s)$ (Artin [1]); ces séries généralisent les séries du Chapitre I, paragraphe 10; elles satisfont à une équation fonctionnelle analogue à celle à propos de laquelle Artin [7, 8] a généralisé la notion de conducteur aux corps non abéliens. On ne sait pas encore si elles sont entières, ou même uniformes. Ce sont des produits de puissances fractionnaires (>0 ou <0) de séries $L(s, \chi)$ ordinaires. Elles permettent de demontrer le théorème suivant :

K *étant galoisien par rapport à* k *de groupe de Galois* G; σ *un élément de* G; h *le nombre de ceux des éléments* $\tau\sigma\tau^{-1}$ *qui sont différents* (τ *quelconque dans* G), n *l'ordre de* G, *il y a une infinité d'idéaux premiers* $\mathfrak{p}$ *de* k *tels que, pour un de leurs facteurs premiers* $\mathfrak{P}$ *dans* K, *on ait* $\left[\frac{K/k}{\mathfrak{P}}\right] = \sigma$, *et l'on a*

$$\lim_{s=1} \frac{\sum \frac{1}{N\mathfrak{p}^s}}{s-1} = \frac{h}{n},$$

la somme étant étendue à ces idéaux premiers ($N\mathfrak{p}$ = *norme absolue de* $\mathfrak{p}$.)

Les méthodes de Landau [1] permettent de démontrer que

$$\mathfrak{N}(x) = \frac{n}{h}\int_2^x \frac{du}{\log u} + O(x\, e^{-\alpha\sqrt{\log x}}),$$

$\mathfrak{N}(x)$ étant le nombre de ceux de ces idéaux $\mathfrak{p}$ tels que $N\mathfrak{p} < x$, α une constante.

C'est une précision d'un théorème de Frobenius [1]. Il généralise le théorème général de la progression arithmétique (Chap. I, § 10_5) comme on le voit en tenant compte de la loi de réciprocité de Artin. *Voir* des démonstrations directes dans Hasse ([4, p. 126 sqq.]; Tchebotareff [1], Schreier [1]).

3. Signalons enfin les deux théorèmes suivants qui montrent combien le cas non abélien diffère du cas abélien :

a. K *étant un sur-corps de* k (*non supposé galoisien*); H *un groupe d'idéaux de* k; *supposons que sauf pour un nombre fini d'idéaux premiers :*

1° *Tout idéal premier de* H *se décompose dans* K *en un produit d'idéaux du premier degré* (*par rapport à* k);

2° *Tout idéal premier de* k *divisible par un idéal premier de* K *du premier degré par rapport à* k, *est dans* H.

Alors K *est corps de classes sur* k *pour le groupe d'idéaux* H (Hasse [2, p. 16]).

b. K *étant un sur-corps galoisien de* k, *non abélien, il y a un nombre* α *et un idéal premier* $\mathfrak{p}$ *tel que* α *ne soit pas reste normique* (*mod* $\mathfrak{p}^x$) *pour un* x *convenable et que* α *soit reste normique pour toute puissance de tout autre idéal premier.*

Le théorème est une réciproque de la loi de réciprocité de Hilbert, qui montre en effet qu'un tel phénomène est impossible dans le cas d'un sur-corps abélien.

APPENDICE.

LES PROGRÈS RÉCENTS DE LA THÉORIE DES NOMBRES.

Par M. Claude CHEVALLEY.

Nous nous proposons ici de donner un rapide aperçu sur les progrès de la théorie faits depuis la rédaction de Herbrand, progrès dus tant à Herbrand lui-même qu'aux autres arithméticiens.

1. **Généralisation de la démonstration directe de l'« Umkehrsatz » au cas « cyclique de degré quelconque ».** — Comme le prévoyait Herbrand, on a pu simplifier considérablement la démonstration de l'« Umkehrsatz » (Chap. II, § IV$_1$) en le démontrant directement pour les extensions relativement cycliques de degré quelconque, sans passer par l'intermédiaire des extensions de degré premier $\mathfrak{l}$ sur un corps contenant les racines ($\mathfrak{l}$-ièmes) de l'unité. On emploie (Chevalley [4]) la même méthode que celle exposée au Chapitre II, paragraphe V. La difficulté réside dans le calcul des nombres a, h_1. Pour a, on peut la résoudre au moyen d'un théorème général sur le groupe des unités d'un sur-corps relativement galoisien, démontré par Herbrand [6] (simplification dans Artin [10]) et d'un mode de raisonnement auquel Herbrand a donné la forme d'un lemme de théorie des groupes, connu sous le nom de lemme de Herbrand. Le calcul de h_1 est, dans une certaine mesure, parallèle à celui de a, les unités d'un corps de nombres $\mathfrak{p}$-adiques remplaçant les unités d'un corps de nombres algébriques, le théorème de Herbrand étant remplacé par un théorème de Deuring sur l'existence d'une base minima d'une extension galoisienne formée des conjugués d'un élément. Ce calcul est d'ailleurs équivalent à la démonstration de l'« Umkehrsatz » dans le cas cyclique pour les corps de nombre $\mathfrak{p}$-adiques.

On arrive de cette manière à démontrer d'une manière relativement simple les faits suivants : k étant un corps de nombres algébriques, K une extension de k de degré m et cyclique, $\mathfrak{f}$ un certain module de k (ne contenant d'ailleurs que des idéaux ramifiés

dans K), H le groupe associé à K (mod $\mathfrak{f}$), l'indice h de H est multiple de m; de plus, l'égalité $h = m$ entraîne le théorème normique de Hasse (Chap. IV, § IV_{3d}).

A partir de là, on peut développer la théorie du corps de classes de deux manières assez différentes.

2. Méthode de Artin [9]. — C'est la plus rapide des méthodes actuelles.

L'inégalité transcendante $h \leqq m$ permet d'abord de démontrer l'« Umkehrsatz » pour les extensions relativement cycliques. On introduit alors une nouvelle définition du corps de classes équivalente à celle de Takagi, en remplaçant la condition b par la suivante :

b'. Presque tous les idéaux premiers de H *se décomposent complètement dans* K.

« Presque tous » est défini de la manière suivante : on dit que presque tous les idéaux premiers d'une certaine catégorie possèdent la propriété P quand on a

$$\lim_{s=1} \frac{}{\log(s-1)} \sum \frac{1}{\mathrm{N}\mathfrak{p}^s},$$

la somme étant étendue aux idéaux premiers de la catégorie considérée qui ne possèdent pas la propriété P.

Au moyen de cette définition, on démontre le théorème de composition (Chap. II, § IV_6), et le théorème de translation (Ch. IV, § III_a) sous les formes suivantes :

Si K, K' *sont corps de classes sur* k *pour les groupes* H, H', KK' *est corps de classes pour le groupe* [H, H'] *et* [K, K'] *est corps de classes pour le groupe* HH'.

Si K *est corps de classes sur* k *pour le groupe* H, *et si* Ω *est un sur-corps quelconque de* k, KΩ *est corps de classes sur* Ω *pour le groupe des idéaux de* Ω *premiers au conducteur de* K/k *dont les normes par rapport à* k *tombent dans* H.

Ceci entraîne en particulier le théorème d'unicité : il existe au plus un corps de classes pour un groupe donné. D'autre part, comme

nous savons déjà que les corps cycliques sont corps de classes, nous avons démontré dans sa généralité l'« Umkehrsatz ».

Artin démontre ensuite le théorème de décomposition (Chap. II, § IV_5), en démontrant d'abord que, non seulement presque tous, mais tous les idéaux premiers du groupe H, pour lequel un corps K est corps de classes se décomposent complètement dans K. La méthode est analogue à celle de la démonstration de la loi de réciprocité (composition de K avec un corps circulaire).

De là, on déduit facilement le théorème d'isomorphie (Chap. II, § IV_2), et en particulier, que tout corps de classes est relativement abélien.

3. **Méthode de Chevalley.** — Elle vise à réduire au minimum la part des méthodes transcendantes dans la théorie.

K étant un sur-corps relativement abélien de k, on introduit le groupe de Artin, qui est le groupe des idéaux $\mathfrak{a}$ de k premiers au discriminant de K/k, et pour lesquels le symbole $\left(\frac{K}{\mathfrak{a}}\right)$ est égal à 1. Il est clair que si H désigne ce groupe, le théorème de décomposition (Chap. II, § IV_5) est vrai. D'autre part, si A est le groupe de tous les idéaux de k premiers au discriminant de K/k, l'inégalité arithmétique $h \geqq m$ permet de démontrer que A/H est isomorphe au groupe de Galois de K/k. Si H représente le groupe de Artin, l'énoncé de la loi de réciprocité (Chap. III, § I) est vrai.

On dit que K est corps de classes sur k si le groupe de Artin coïncide avec le groupe de congruence attaché à K dans k. Par une méthode inspirée de celle de la démonstration de la loi de réciprocité, on peut démontrer arithmétiquement que si les corps relativement circulaires sont corps de classes, il en est de même des corps cycliques quelconques, puis des corps abéliens quelconques. Par contre, pour démontrer que les corps circulaires sont corps de classes, on ne peut pas encore éviter l'emploi des moyens transcendants.

Cette méthode conduit, en même temps qu'aux théorèmes de la théorie du corps de classes, à la loi de réciprocité.

4. **Théorème d'existence.** — Le fait que l'on puisse démontrer

entièrement l'« Umkehrsatz » avant de démontrer le théorème d'existence, permet de simplifier notablement la démonstration de ce dernier. C'est ce qui fut fait simultanément par Herbrand [5] et Chevalley [4], [5].

La méthode est la suivante : Étant donné dans un corps k un groupe de congruence H tel que, si n est l'ordre d'un élément quelconque du groupe quotient par H du groupe des idéaux de k premiers au conducteur de H, k contienne les racines $n^{\text{ièmes}}$ de l'unité, on construit un groupe H_1 contenu dans H et pour lequel on démontre l'existence d'un corps de classes K_1. La loi de réciprocité permet alors de démontrer qu'il existe un corps de classes K pour H. Pour démontrer l'existence de K_1, on construit, en même temps que H_1, un autre groupe H_2 tel que tous les idéaux premiers divisant n et les idéaux premiers à l'infini divisent le conducteur de l'un ou l'autre des groupes H_1, H_2; on construit également les corps K_1, K_2 composés des corps kummériens $k(\sqrt[n]{\omega})$ dont les groupes attachés peuvent contenir H_1 ou H_2. On sait que K_1, K_2 sont corps de classes sur k pour des groupes H'_1, H'_2 qui contiennent respectivement H_1, H_2. D'autre part, un calcul de théorie des groupes conduit à l'égalité $(A_1 : H_1)(A_2 : H_2) = (A_1 : H'_1)(A_2 : H'_2)$ où A_1, A_2 sont les groupes des idéaux de k premiers aux conducteurs de H_1, H_2. On en déduit $H_1 = H'_1$, $H_2 = H'_2$, ce qui démontre le théorème.

Il est ensuite facile, au moyen d'un lemme basé sur la loi de réciprocité, de passer au cas où k ne contient pas les racines de l'unité nécessaires à la démonstration précédente.

5. **Méthodes empruntées à l'algèbre hypercomplexe.** — Le lien entre l'algèbre hypercomplexe et la théorie du corps de classes est très étroit. Par exemple, le théorème normique de Hasse (Chap. IV, § IV_{3d}) s'interprète de la manière suivante : « si une algèbre simple A, cycliquement représentable, de centre k, est telle que pour tous les idéaux premiers finis ou infinis $\mathfrak{p}$, $A_{\mathfrak{p}}$ se décompose complètement, A est elle-même complètement décomposée ».

D'une manière plus précise, Hasse [28], [29] a attaché à une algèbre simple de centre k une infinité d'invariants, définis chacun pour un idéal premier de k, qui sont des nombres fractionnaires (mod 1), et dont seulement un nombre fini est différent de 0. Ces nombres forment un système complet d'invariants, et la somme de

tous ces invariants est toujours nulle. Cette dernière propriété est une traduction de la loi de réciprocité de Hilbert.

Ces théorèmes sur les algèbres ont d'abord été établis au moyen de la théorie du corps de classes. Mais on peut (Zorn [1]), démontrer directement le théorème fondamental énoncé plus haut, et à partir de là, construire la théorie du corps de classes d'une manière très élégante (Hasse [29]).

6. **La théorie des corps galoisiens.** — La thoérie des restes normiques dans les extensions galoisiennes a été approfondie par Hasse [26] qui étudie la croissance avec n de l'indice des restes normiques HH' (mod $\mathfrak{p}^n$) d'une extension galoisienne, $\mathfrak{p}$ étant un idéal premier quelconque. Il en tire une démonstration simple du théorème sur la différente (Chap. IV, § II_2).

D'autre part, on a essayé d'étendre, grâce aux méthodes de l'algèbre hypercomplexe, la théorie du corps de classes aux extensions galoisiennes. Le résultat le plus important dans cette voie est dû à Mlle Nœther, qui étend au cas galoisien le théorème du genre principal (Nœther [1]). On a également donné des lois de décomposition (Hasse [29], Artin), mais la difficulté n'est pas encore résolue. Notamment, on n'a encore rien d'analogue au théorème d'isomorphie, ni au théorème d'existence.

7. **Le théorème des idéaux principaux.** — La démonstration très compliquée donnée par Fürtwangler a été simplifiée d'abord par Magnus [1], puis par Iyanaga [2].

INDEX BIBLIOGRAPHIQUE.

La bibliographie ci-dessous ne vise pas à être complète; n'y sont indiqués que les ouvrages ayant un rapport direct avec les points traités dans ce fascicule. On trouvera une bibliographie complète :

a. Pour la théorie générale des corps algébriques avant 1896, dans HILBERT [1];
b. *Id.*, entre 1896 et 1911, dans FUETER [1];

c. Pour la théorie du corps de classes et des lois de réciprocité, dans HASSE [4] (il faut ajouter les ouvrages principaux indiqués dans HASSE [2] et qui sont également cités ci-dessous).

ARTIN. — 1. Ueber die Zetafunktion gewisser algebraischer Zahlkörper (*Math. Ann.*, t. 89, 1923, p. 147-156).

— 2. Ueber eine neue Art von L.-Reihen (*Hamb. Abh.*, t. 3, 1924, p. 89-108).

— 3. Ueber den zweiten Ergänzungsgesetz der l-ten Potenzreste im Körper $k(\zeta)$ der l-ten Einheitswurzeln und in Oberkörper von $k(\zeta)$ (*Journal für Math.*, t. 154, 1925, p. 143-148; avec Hasse).

— 4. Beweis des Allgemeines Reciprozitätsgesetzes (*Hamb. Abh.*, t. 5, 1927, p. 353-363).

— 5. Die beiden Ergänzungssätze zum Reciprozitätsgesetz der l-ten Potenzreste im Körper der l-ten Einheitswurzeln (*Hamb. Abh.*, t. 6, 1928, p. 146-162; avec Hasse).

— 6. Idealklassen im Oberkörper und allgemeines Reciprozitätsgesetz (*Hamb. Abh.*, t. 7, 1930, p. 46-51).

— 7. Zur Theorie der L-Reihen mit allgemeinen Gruppencharakteren (*Hamb. Abh.*, t. 8, 1931, p. 292-306).

— 8. Die gruppentheoretische Struktur der Diskriminant algebraischer Zahlkörper (*Journal für Math.*, t. 164, 1931, p. 1-11).

— 9. Vorträge über Klassenkörpertheorie, 1932, polycopié, Séminaire de Göttingen.

— 10. Ueber Einhechen relativ galoisscher Zahlkörper (*Journal für math.*, t. 167, 1932, p. 153).

BURNSIDE. — 1. The theory of groups (Cambridge, 1911, 2e édition).

CHEVALLEY. — 1. Sur un théorème de M. Hasse (*C. R. Acad. Sci.*, t. 191, 1930, p. 369).

— 2. Sur la théorie des restes normiques (*C. R. Acad. Sci.*, t. 191, 1930, p. 426).

— 3. Relation entre le nombre des classes d'un sous-corps et celui d'un sur-corps (*C. R. Acad. Sc.*, 192, 1931, p. 257).

— 4. La théorie du corps de classes dans les corps finis et les corps locaux (Thèse) (*Journ. of the Faculty of Sciences*, Tokyo, 1933, p. 365).

— 5. Nouvelle démonstration du théorème d'existence en théorie du corps de classes (avec J. Herbrand) (*C. R. Acad. Sc.*, 192, 1931, p. 814).

— 6. Sur la structure de la théorie du corps de classes (*C. R. Acad. Sc.*, 1932).

DEBEKIND et WEBER. — Theorie der algebraischen Funktionen einer Veränderlichen (*Journal für Math.*, t. 92, 1883, p. 180-290).

FROBENIUS. — 1. Ueber Beziehungen zwischen den Primidealen eines algebraischen Körpers und den Substitutionen seiner Gruppe (*Sitzungsber. der Preus. Akad. der Wiss. Berlin*, 1896, p. 689-703).

FUETER. — 1. Die Klassenkörper der komplexen Multiplication, und ihr Einfluss auf die Entwicklung der Zahlentheorie (*Jahresber. der Deusch. Math. Ver.*, t. 20, 1911, p. 1-47).

— 2. Vorlesungen über die Singularen Moduln und die Komplexe Multiplikation der elliptischen Funktionen (Leipzig, 1924).

— 3. Reciprozitätsgesetz im quadratich imaginaren Zahlkörper (*Göttinger Nachr.*, 1927, p. 336-346 et 427-445).

FURTWÄNGLER. — 1. Die Konstruktion des Klassenkörpers für solche algebraischen Zahlkörper die eine l te Einheitswurzel enthalten, und deren Idealklassen eine zyklische Gruppe von Grad l bilden (*Gött. Nachr.*, 1903, p. 202-217).

— 2. Ueber die Konstruktion des Klassenkörper für beliebige algebraische Zahlkörper die eine l te Einheitswurzel enthalten (*Gött. Nachr.*, 1903, p. 282-303).

— 3. Die Konstruktion des Klassenkörpers für beliebige algebraische Zahlkörper (*Gött. Nachr.*, 1904, p. 174-195).

— 4. Ueber das Reciprozitätsgesetz der l-ten Potenzreste in algebraischen Zahlkörpern wenn l eine ungarade Primzahl bedeutet (*Math. Ann.*, t. 58, 1904, p. 1-49).

— 5. Ueber die Klassenzahlen Abelscher Zahlkörper (*Journal für Math.*, t. 134, 1908, p. 91-94).

— 6. Das Reciprozitätsgesetz für Potenzreste mit Primzahlexponenten (*Math. Ann.*, (1), t. 67, 1909, p. 1-20; (2), t. 72, 1912, p. 346-386; (3), t. 74, 1913, p. 413-429).

— 7. Letzter Fermat'scher Satz und Eisensteinsches Reziprocitätsgesetz (*Wiener Akad. Ber.*, p. 589-592).

— 8. Ueber das Verhalten der Ideale des Grundkörpers im Klassenkörper (*Monatshefte für Math. und Ph.*, t. 27, 1916, p. 1-15).

— 9. Ueber das Reciprozitätsgesetz für Primzahlexponente (*Journal für Math.*, t. 157, 1927, p. 15-28).

— 10. Ueber das Reciprozitätsgesetz für ungerade Primzahlexponente (*Math. Ann.*, t. 98, 1928, p. 539-543).

— 11. Beweis des Hauptidealsatzes für die Klassenkörper algebraischer Zahlkörper (*Hamb. Abh.*, t. 7, 1930, p. 14-36).

HASSE. — 1. *Höhere Algebra*, 2 vol. (Sammlung Gösschen., Berlin, 1926).

— 2. Bericht über neuere Untersuchungen und Problem aus der Theorie der algebraischen Zahlkörper (*Jahresber. der Deutsch. Math. Ver.*, Teil I : Klassenkörpertheorie, 1926, p. 1-55).

— 3. *Id.*, Teil I *a* : Beweise zu Teil I, t. 36, 1927, p. 255-311. Il existe de ces deux derniers ouvrages un tirage en un seul volume. Les numéros de page se rapporteront à ce tirage; on en déduira sans peine les numéros de pages correspondants des mémoires isolés.

— 4. *Id.*, Teil II : Reciprozitätsgesetz, Ergänzungsband, VI, 1930, p. 1-204.

— 5. Ueber die Normenreste eines relativ-zyklischen Körper vom Primzahlgrad l nach einem Primteiler von l (*Math. Ann.*, t. 90, 1923, p. 262-278; avec Hensel).

— 6. Zerlegungs- und Vertauschungssätze für das Hilbertsche Normenrestsymbol (*Journal für Math.*, t. 154, 1925, p. 20-35).

— 7. Zur Theorie des quadratischen Hilbertschen Normenrestsymbols in algebraischen Zahlkörpern (*Journal f. Math.*, t. 153, 1924, p. 76-92).

— 8. Zur Theorie des Hilbertschen Normenrestsymbol in algebraischen Zahlkörpern (*Journal für Math.*, t. 153, 1924, p. 184-191; t. 154, 1925, p. 174-177).

— 9. Das allgemeine Reciprozitätsgesetz und seine Ergänzungssätze in beliebigen algebraischen Zahlkörpern für gewisse nicht-primäre Zahlen (*Journal für Math.*, t. 153, 1924, p. 192-207).

— 10. Ueber das allgemeine Reciprozitätsgesetz der l-ten Potenzreste im Körper $k(\zeta)$ der l-ten Einheitzwurzel und in Oberkörpern von $k(\zeta)$ (*Journal für Math.*, t. 154, 1925, p. 96-109).

— 11. Ueber den zweiten Ergänzungssatz zum Reciprozitätsgesetz der l-ten Potenzreste in Körper $k(\zeta)$ der l-ten Einheitswurzeln und in Oberkörpern von $k(\zeta)$ (*Journal für Math.*, t. 154, 1925, p. 143-148; avec Artin).

— 12. Das allgemeine Reciprozitätsgezetz der l ten Potenzreste für beliebige, zu l prime Zahlen, in gewissen Oberkörpern des Körpers der l-ten Einheitswurzeln (*Journal für Math.*, t. 154, 1925, p. 199-215).

— 13. Der zweite Ergänzungssatz zum Reciprozitätsgesetz der l-ten Potenzreste für beliebige zu l prime Zahlen in gewissen Oberkörpern des Körpers der l-ten Einheitswurzeln.

— 14. Das Eisensteinsche Reciprozitätsgesetz der n-ten Potenzreste (*Math. Ann.*, t. 97, 1927, p. 599).

— 15. Ueber das Reciprozitätsgesetz der m-ten Potenzreste (*Journal für Math.*, t. 158, 1927, p. 228-259).

— 16. Die beiden Ergänzungssätze zum Reciprozitätsgesetz der l-ten Potenzreste im Körper der l-ten Einheitswurzeln (*Hamb. Abh.*, t. 6, 1928, p. 146-162); avec Artin).

— 17. Zum expliciten Reciprozitätsgesetz (*Hamb. Abh.*, t. 7, 1930, p. 52-63).

— 18. Arithmetische Theorie der kubischen Zahlkörper auf klassenkörpertheoretischer Grundlage (*Math. Zeits.*, t. 31, 1930, p. 565-582).

— 19. Ein Satz über relativ-Galoischer Zahlkörper (*Math. Zeits.*, t. 31, 1930, p. 559-561).

— 20. Neue Begründung und Verallgemeinerung der Theorie des Normenrestsymbols (*Journal für Math.*, t. 162, 1930, p. 134-144).

— 21. Die Normenresttheorie relativ Abelscher Zahlkörper als Klassenkörpertheorie im kleinen (*Journal für Math.*, t. 162, 1930, p. 145-154).

— 22. Führer, Diskriminante und Verzweigungsgruppen relativ-Abelscher Zahlkörper (*Journal für Math.*, t. 162, 1930, p. 169-184).

— 23. Neue Begründung der komplexen Multiplication (*Journal für Math.*, t. 157, 1927, p. 115-139).

— 24. Ueber die Einzigkeit der beiden fundamentalsätze der elementarer Zahlentheorie (*Journal für Math.*, t. 155, 1926, p. 199-220).

— 25. Klassenkörpertheorie, cours polycopié, 1933, Séminaire mathématique de Marburg.

— 26. Théorie des restes normiques dans les extensions galoisiennes (*C. R. Acad. Sc.*, t. 197, 1933, p. 469), et Application au cas abélien de la théorie des restes normiques dans les extensions galoisiennes (*C. R. Acad. Sc.*, t. 197, 1933, p. 511).

— 27. Ueber $\mathfrak{p}$ adische Schiefkörper und ihre Bedeutung für hyperkomplexer Zahlentheorie (MA, 104).

— 28. Theory of cyclic algebras over an algebraic number field (*Trans. of the Amer. Math. Soc.*, t. 34, 1, p. 171).

— 29. Die Struktur der R. Brauerschen Algebrenklassengruppe über einem algebraischen Zahlkörper (MA, t. 107, 1933).

— 29. Beweis eines Hauptsatzes in der Theorie der Algebren, avec R. Brauer et Mlle Nœther (*Journ. für Math.*, t. 167, 1931).

HECKE. — 1. Vorlesungen über die Theorie der algebraischen Zahlen (Leipzig, 1923).

— 2. Höhere Modulfunktionen und ihre Anwendungen an der Zahlentheorie (*Math. Ann.*, t. 71, 1912, p. 1-57).

— 3. Eien neue Art von zeta-Funktionen und ihre Beziehungen zur Verteilung der Primzahlen (*Math. Zeits.*, t. 1, 1918, p. 357-376; t. 6, 1920, p. 11-51).

HENSEL. — 1. Zahlentheorie (Berlin Leipzig, 1913).

— 2. Die exponential Darstellung der Zahlen eines algebraischen Zahlkörpers für den Beriech eines Primdivisors (H. A. Schwarz-Festschrift, Berlin, 1914, p. 61-75).

— 3. Untersuchung der Zahlen eines algebraischen Körpers für den Bereich eines Primteilers (*Journ. für Math.*, t. 145, 1915, p. 92-113).

— 4. Die multiplikative Darstellung der algebraischen Zahlen für den Bereich eines Primteilers (*Journal für Math.*, t. 146, 1916, p. 190-215).

— 5. Eine neue Theorie der algebraischen Zahlen (*Math. Zeits.*, t. 2, 1918),

— 6. Zur multiplikativen Darstellung der algebraischen Zahlen für den Bereich eines Primtellers (*Journal für Math.*, t. 151, 1921, p. 210 212).

— 7. Ueber die Normenreste und Nichtreste in den allgemeinen relativ-Abel'schen Zahlkörpern (*Math. Ann.*, t. 85, 1922, p. 1-10).

HERBRAND. — 1. Sur la théorie des groupes de décomposition, d'inertie et de ramification (*Journal de Liouville*, 1931).

— 2. Sur les classes des corps circulaires (*Journal de Liouville*, 1932, p. 417).

— 3. Sur les théorèmes du genre principal et des idéaux principaux (*Hamb. Abh.*, t. 9, p. 84).

— 4. Sur une propriété du discriminant des corps algébriques (*Annales de l'École Normale*, 1932, p. 105).

— 5. Nouvelle démonstration du théorème d'existence en théorie du corps de classes, avec Chevalley (*C. R. Acad. Sc.*, 1931, p. 814).

— 6. Nouvelle démonstration et généralisation d'un théorème de Minkowski (*C. R. Acad. Sc.*, t. 191, 1930, p. 1282).

HILBERT. — 1. Die Theorie der algebraischer Zahlkörper (« Zahlbericht ») (*Jahresber. der Deuts. Math. Ver.*, t. 4, 1897, p. 177-546). Traduction française aux *Annales de Toulouse*, édité également à part (Hermann, Paris).

— 2. Ueber die Theorie des relativ-quadratischen Zahlkörpers (*Math. Ann.*, t. 51, 1899, p. 1-127).

— 3. Ueber die Theorie der relativ-Abelschen Zahlkörper (*Gött. Nachr.*, 1898, p. 370-399; ou *Acta Math.*, t. 26, 1902, p. 99-131).

— 4. Mathematische Probleme (*Gött. Nachr.*, 1900, p. 253-297).

IYANAGA. — 1. Ueber der allgemeinen Hauptidealsatz (*Jap. Journ. of Math.*, t. 7, 1931.

— 2. Zum Beweis des Hauptidealsatzes, Abhand. Hamb.

LANDAU. — 1. Ueber Ideale und Primideale in Idealklassen (*Math. Zeits.*, t. 2, 1918, p. 52-154).

ORE. — 1. Newtonsche Polygone und algebraische Zahlkörper (*Math. Ann.*, t. 99, 1928, p. 84-117).

MORYIA. — 1. Ueber die Klassenzahl eines relativ zyklischen Zahlkörpers vom Primzahlgrad (*Proc. of Imp. Ac. of Japan*, t. 6, 1930, p. 245-247).

NOETHER. — 1. Der Hauptgechlechtsatz für relativ-galoische Zahlkörper, MA, t. 108, 1933.

POLLACZEK. — 1. Ueber die Einheiten Relativ-Abelscher Zahlkörper (*Math. Zeits.*, t. 30, 1929, p. 520-551).

SCHMIDT (F. K.). — 1. Zur Klassenkörpertheorie im kleinen (*Journal für Math.*, t. 162, 1930, p. 154-168).

SCHOLZ. — 1. Zur Klassenkörpertheorie auf Takagischer Grundlage (*Math. Zeits.*, t. 29, 1929, p. 60-69; avec Hasse).

— 2. Zwei Bemerkungen zum Klassenkörperturm (*Journal für Math.*, t. 161, 1929, p. 200-207).

— 3. Ueber das Verhältnis von Idealklassen und Einheitengruppe in Abelscher Zahlkörpern vom Primzahlpotenzgrad (*Heiselberger Akad. Ber.*, 1930, Art. 17, p. 31-55).

SCHREIER. — 1. Ueber eine Arbeit von Herrn Tchebotareff (*Hamb. Abh.*, t. 5, 1927, p. 1-6).

SIEGEL. — 1. Neuer Beweis für die Funktionalgleichung der Dedekindchen Zétafunktion (*Math. Ann.*, t. 85, 1922, p. 123-128).

SPEISER. — 1. Die Theorie der Gruppen von endlicher Ordnung (Berlin, 1927).

— 2. Die Zerlegungsgruppe (*Journal für Math.*, t. 149, 1919, p. 174-188).

STEINITZ. — 1. Algebraische Theorie der Körper (*Journal für Math.*, t. 137, 1910, p. 167-309).

TAKAGI. — 1. Ueber eine Theorie des relativ Abelscheh Zahlkörpers (*Journal of the Col. of. Sc. of Tokyo*, t. 41, 1920, Art. 9, p. 1-133).

— 2. Ueber das Reciprozitätsgesetz in einem beliebigen algebraischen Zahlkörper (*Journal of the Col. of Sc. of Tokyo*, t. 44, 1922, Art. 5, p. 1-50).

— 3. On the law of reciprocity in the cyclotomic Corpus (*Proc. of the Ph. Math. Soc. of Japan*, 1922).

— 4. Zur Theorie des Kreiskörpers (*Journal für Math.*, t. 157, 1927, p. 230-238; reproduction du précédent avec des compléments).

TCHEBOTAREFF. — 1. Die Bestimmung der Dichtigkeit einer Menge von Primzahlen welche zu einer gegebenen Substitutionsklasse gehören (*Math. Ann.*, t. 95, 1926, p. 191-228).

— 2. Zur Gruppentheorie des Klassenkörpers (*Journal für Math.*, t. 161, 1930, p. 179-183).

VAN DER WAERDEN. — 1. Ein logarithmenfreier Beweis des Dirichletschen Einheitensatzes (*Hamb. Abh.*, t. 6, 1928, p. 259-262), 2 vol. — 2. Moderne Algebra.

WEBER. — 1. Lehrbuch der Algebra, vol. 3, 2e édition (Braunschweig, 1908).

— 2. Ueber Zahlengruppen in algebraischen Körpern (*Math. Ann.*, t. 48, 1897, p. 433-473).

— 3. *Id.*, t. 49, 1897, p. 83-100.

— 4. Ueber zyklische Zahlkörper (*Journ. für Math.*, t. 132, 1907, p. 167-188).

ZORN. — Note zur analytichen hypercomplexen Zahlentheorie (*Hamb. Abh.*)

UNIVERSITÉ DE GRENOBLE I
LABORATOIRE
DE MATHÉMATIQUES PURES
INSTITUT FOURIER

TABLE DES NOTIONS.

Nous indiquons ci-dessous le paragraphe du Chapitre I où se trouve la définition du terme :

Abélien (Corps —) ..... 3_2
» (Groupe —) ..... 1_4
Absolu (Degré —) ..... 2_3
» (Norme —) ..... 3_1
» (Norme — d'un idéal) ..... 5_8
Algébrique (Entier —) ..... 4_1
» (Nombre —) ..... 2_1
Attaché (Groupe — à un corps) ..... 10_5
Automorphisme ..... 3_2
Base (d'un groupe abélien) ..... 1_4
Caractère ..... 1_5
» propre ..... 7_6
» (Conducteur du —) ..... 7_6
Classe ..... 5_6
» au sens ordinaire ..... 7_4
» au sens restreint ..... 7_4
Commutateurs ..... 1_6
Complexe ..... 1_3
Conducteur ..... 7_5
Conjugué (Groupe —) ..... 1_3
» correspondant ..... 3_1
Congru (par rapport à un groupe) ..... 1_3
Congruence (Classe de —) ..... 7_2
Corps ..... 2_1
Cyclique (Groupe —) ..... 3_2
» (Corps —) ..... 1_4
Décomposition (Groupe de —) ..... 9_1
Défini (Groupe — suivant un idéal) ..... 7_4
Degré (d'un corps) ..... 2_3
» (d'un idéal premier) ..... 5_8
Différente ..... 8_1
Direct (Produit —) ..... 1_7
Discriminant ..... 8_1
Entier ..... 4_1
» (Idéal —) ..... 5_1
» (Idéal — pour) ..... 7_2
Fini (Groupe —) ..... 1_1

Fini (Idéal —) ..... 7_3
Galois (Groupe de —) ..... 3_3
Généralisé (Discriminant —) ..... 8_3
» (Idéal —) ..... 7_3
Groupe ..... 1_1
» quotient ..... 1_3
» d'idéaux ..... 7_2
Holoédriquement (— isomorphe) ..... 1_2
Idéal ..... 5_1
Imaginaire (Corps —) ..... 2_1
Indice (d'un groupe d'idéaux) ..... 7_4
Inertie (Groupe d' —) ..... 9_1
Infini (Idéal —) ..... 7_3
Invariant (Sous-groupe —) ..... 1_3
Irréductible (Polynome —) ..... 2_2
Isomorphie ..... 1_2
Mériédriquement (— isomorphe) ..... 1_2
Norme (d'un nombre) ..... 3_1
» (d'un idéal) ..... 5_8
Ordre (— d'un groupe) ..... 1_1
» (— d'un élément) ..... 1_4
Premier (Idéal —) ..... 5_5
» (Idéal — pour) ..... 7_2
Principal (Caractère —) ..... 1_5
» (Idéal —) ..... 5_2
Produit (d'idéaux) ..... 5_3
Ramification (Groupe de —) ..... 9_1
Ramifié (Corps —) ..... 8_3
» (Idéal —) ..... 5_7
» (Idéal infini —) ..... 8_3
Rayon ..... 7_4
Réel (Corps —) ..... 2_1
Relatif (Degré —) ..... 2_3
Sous-corps ..... 2_5
Sous-groupe ..... 1_3
Sur-corps ..... 2_3
Totalement positif (Nombre —) ..... 7_3
Unité (d'un corps) ..... 6_1
» (d'un groupe) ..... 1_1
» (Idéal —) ..... 5_3

Dans le cours du texte, les chiffres entre crochets renvoient à la Bibliographie. Les autres chiffres renvoient aux paragraphes du texte, le chiffre en indice indiquant la subdivision du paragraphe; le numéro du Chapitre n'est indiqué que s'il est différent de celui que l'on est en train de lire.

TABLE DES MATIÈRES.

Pages.

INTRODUCTION 1

CHAPITRE I.

THÉORIE GÉNÉRALE DES CORPS ALGÉBRIQUES.

1. Groupes 3
2. Corps algébriques 7
3. Théorie de Galois 9
4. Entiers 10
5. Idéaux 11
6. Unités 14
7. Congruences 15
8. Différente et discriminant 18
9. Groupe de décomposition, d'inertie, de ramification 19
10. La fonction $\zeta(s)$ et ses généralisations 22
11. Les analogies fonctionnelles et les nombres $\mathfrak{p}$-adiques 25

CHAPITRE II.

LE CORPS DE CLASSES.

1. Le corps circulaire des racines $m^{\text{ièmes}}$ de l'unité 27
2. Corps quadratiques 28
3. Corps kummériens 31
4. Le corps de classes 33
5. Cas du degré relatif premier 36
6. Cas général 39

CHAPITRE III.

LOIS DE RÉCIPROCITÉ.

1. Loi de réciprocité de Artin 40
2. Loi de réciprocité de Hasse 41
3. Loi de réciprocité de Hilbert 43
4. Lois explicites de réciprocité 45
7. Application au théorème de Fermat 46

CHAPITRE IV.

APPLICATIONS.

Pages.
1. Cas particuliers 47
2. Différente et groupe de ramification 49
3. Passage à un sur-corps 50
4. Applications diverses 51
5. Corps non abéliens 54

APPENDICE.

LES PROGRÈS RÉCENTS DE LA THÉORIE DES NOMBRES.

1. Généralisation de la démonstration directe de l' « Umkehrsatz » au cas « cyclique de degré quelconque » 57
2. Méthode de Artin 58
3. Méthode de Chevalley 59
4. Théorème d'existence 59
5. Méthodes empruntées à l'algèbre hypercomplexe 60
6. La théorie des corps galoisiens 61
7. Le théorème des idéaux principaux 61

97519 Paris. — Imp. GAUTHIER-VILLARS, quai des Grands Augustins, 55.